NIST Special Publication 800-53A

Guide for Assessing the Security Controls in Federal Information Systems

Building Effective Security Assessment Plans

Ron Ross
Arnold Johnson
Stu Katzke
Patricia Toth
Gary Stoneburner
George Rogers

I N F O R M A T I O N S E C U R I T Y

THIRD PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Notes to Reviewers

In this third public draft of NIST Special Publication 800-53A, the authors have attempted to streamline the security assessment procedures and provide additional guidelines to make the assessment process more efficient and cost-effective. The authors anticipate the content of this publication will be incorporated into automated support tools and have therefore, structured the assessment procedures to facilitate such application. Key changes to NIST Special Publication 800-53A include:

- A new format for assessment procedures that focuses on assessment objectives expressed as determination statements;
- Assessment procedures updated to be consistent with NIST Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*;
- A new extended assessment procedure that is intended to increase the grounds for confidence in security control effectiveness, is linked directly to the impact level of the information system under assessment, and eliminates some of the redundancies in previous assessment procedures;
- A direct linkage of the assessment procedures in NIST Special Publication 800-53A to the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) suite under development to facilitate faster, more reliable, and more cost-effective assessments of security controls employed within information systems;
- Options for reducing the assessment requirements for low-impact and moderate-impact information systems;
- New guidelines for—
  - establishing policies and procedures for security control assessments;
  - identifying roles and responsibilities of managers and assessors;
  - selecting appropriate security controls to be assessed;
  - addressing the depth and coverage of security assessments;
  - determining the frequency of periodic assessments;
  - conducting penetration testing on information systems;
  - describing linkages to other evaluation and testing activities to include reusing assessment evidence, when appropriate; and
  - developing assessment strategies for common (infrastructure-related) security controls.
- A new assessment reporting form and an approach for managing assessment results, defining next steps in the remediation process, and providing meaningful security status information to authorizing officials.

Comments on this public draft will be accepted through **July 31, 2007**. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert@nist.gov. The FISMA Implementation Project main website at http://csrc.nist.gov/sec-cert contains information on all of the FISMA-related security standards and guidelines and how the publications can be used to manage enterprise risk and build a comprehensive information security program.

-- RON ROSS
PROJECT LEADER, FISMA IMPLEMENTATION PROJECT

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. However, it may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-53A, 376 pages

(June 2007) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS JUNE 4 THROUGH JULY 31, 2007.
COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT 100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgements

The authors, Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, Gary Stoneburner, and George Rogers wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks is also extended to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security information and information systems). The agency's risk assessment validates the security control set by determining if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the nation. The resulting set of security controls establishes a level of "security due diligence" for the federal agency and its contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to help ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all required security controls are implemented in agency information systems when determining the tailored and supplemented control baselines described in NIST Special Publication 800-53.

See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on compliance.

Preface

Security assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, they are the last line of defense in knowing the strengths and weaknesses of an organization's information system which is supporting critical federal applications and missions in a global environment of sophisticated threats. The findings produced by security assessors during security assessments are used primarily in determining the overall effectiveness of the security controls in an information system and in providing credible and meaningful inputs to the organization's security accreditation process. A well-executed security assessment helps to determine the validity of the security controls contained in the information system security plan and to facilitate a cost-effective approach to correcting any deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, is a companion guideline to NIST Special Publication 800-53, *Minimum Security Controls for Federal Information Systems*. Each publication provides guidance for implementing the steps in the NIST Risk Management Framework (RMF). Special Publication 800-53 covers the steps in the RMF that address security control selection and supplementation (i.e., determining what security controls are needed to protect organizational operations and assets, individuals, other organizations, and the nation) in accordance with the security requirements stated in FIPS 200. This includes: (i) selecting an initial set of baseline security controls based on a FIPS 199 impact analysis; (ii) tailoring the baseline controls; and (iii) supplementing the controls, as necessary, based on an organizational assessment of risk. Special Publication 800-53A covers both the security control assessment and continuous monitoring steps in the RMF and provides guidance on: (i) how to build an effective security assessment plan; and (ii) how to successfully execute the plan to assess the security controls in an organizational information system.

Prior to the start of a security assessment, the system security plan is agreed upon and approved by key organizational officials. Therefore, security assessments using the procedures provided in this publication are not intended to make judgments on the necessity or sufficiency of the set of security controls documented in the security plan for the information system. Rather the assessment procedures are applied to determine if the agreed-upon and approved security controls (as stated in the security plan and as employed within the information system by the organization during the execution of the RMF) are, in fact, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Assessors, in the course of executing the procedures within NIST Special Publication 800-53A, might discover potential errors or oversights in the security plan and should determine how those potential errors or oversights may affect the confidentiality, integrity, and availability of the information system in the event of a compromise or breach of the system. Such discoveries and determinations, however, are a by-product of the assessment and not the purpose of the assessment. Therefore, while assessors are expected to notify appropriate organizational officials about any potential problems with the system security plan, assessors are not empowered to second-guess or question the decisions of mission/system owners and authorizing officials concerning the impact level of the information system or the security control selection and supplementation activities, which include the tailoring and supplementation of the security control baselines from NIST Special Publication 800-53.

It is expected that organizations will, in some cases, need to tailor and supplement the basic assessment procedures provided in this publication. The concept of tailoring and supplementing used in this document is similar to the concept described in NIST Special Publication 800-53. Tailoring involves scoping the assessment procedures to match the characteristics of the information system under assessment and supplementing involves adding assessment procedures or assessment details to adequately meet the organization's risk management needs. The tailoring of assessment procedures provides organizations with the flexibility needed to avoid overly-constrained assessment approaches. Supplementing includes adding assessment determinations or adding organization-specific details such as, but not limited to, system and platform-specific information for selected security controls employed in the hardware, software, and firmware. This additional assessment or level of detail is left to the discretion of the organization in order to maximize flexibility in developing security assessment plans while applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. A major design objective for NIST Special Publication 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are essential for achieving such consistency. In addition to the assessment framework and initial starting point for assessment procedures, NIST has initiated the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) that is supportive of and complementary to the approach for achieving effective, efficient, and consistent assessments outlined in this publication. The primary purpose of the SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific security configuration settings, thereby reducing vulnerabilities when products are not configured properly. The current version of SCAP is designed to help organizations automate FISMA technical security control compliance activities by regularly scanning information technology products using SCAP product-specific checklists. SCAP checklists have FISMA compliance mappings embedded within the checklist so that SCAP-compatible tools can automatically generate NIST Special Publication 800-53 assessment and compliance evidence. The ultimate objective is to achieve a direct linkage, where appropriate, of the assessment procedures found in NIST Special Publication 800-53A to the SCAP automated testing of information system mechanisms and associated security configuration settings. Future versions of SCAP will likely standardize and automate implementation and change/remediation of security configuration settings and corresponding Special Publication 800-53 security controls. SCAP will help in achieving test results that are more uniform and repeatable, automated test procedures that are more transparent, and greater efficiency for assessment teams. Additional details on the ISAP/SCAP initiative, as well as freely available SCAP reference data, can be found at the NIST website at http://nvd.nist.gov.

Finally, it should be noted that for environments with credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets, additional assurances may be required. NIST Special Publication 800-53 indicates the need for risk acceptance or additional assurances for moderate-impact and high-impact information systems whenever the organization is relying on one or more security controls to mitigate risks from more capable threat sources. In a similar manner, NIST Special Publication 800-53A recognizes that, for such controls, organizationally derived, additional assessment steps will likely be required. These additional assessment steps will include the steps associated with verifying the *Additional Requirements Enhancing Moderate-impact and High-impact Information Systems* in Appendix E of NIST Special Publication 800-53; namely, that the security control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

CAUTIONARY NOTES

Organizations should carefully consider the potential impacts of employing the procedures defined in this Special Publication when assessing the security controls in *operational* information systems. Certain assessment procedures, particularly those procedures that directly impact the operation of hardware, software, and/or firmware components of an information system, may inadvertently affect the routine processing, transmission, or storage of information supporting critical organizational missions or business functions. For example, a key information system component may be taken off line for assessment purposes or a component may suffer a fault or failure during the assessment process. Organizations should take necessary precautions during security control assessment periods to ensure that organizational missions and business functions continue to be supported by the information system and that only approved impacts to operational effectiveness are caused by the assessment.

Security controls have been restated in NIST Special Publication 800-53A for ease of use by assessors in conducting assessments of security controls and should not be viewed as replacing or revising the security controls in Special Publication 800-53 which remains the definitive NIST recommendation for employing security controls in federal information systems.

Unless otherwise stated, all references to NIST publications in this document (i.e., Federal Information Processing Standards and Special Publications) are to the most recent version of the referenced publication.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY CONTROL EFFECTIVENESS IN INFORMATION SYSTEMS

Today's information systems[3] are incredibly complex assemblages of hardware, software, firmware, and people, all working together to provide organizations with the capability to process, store, and transmit information on a timely basis to support various organizational missions and business functions. The degree to which organizations have come to depend upon these information systems to conduct routine and critical missions and business functions means that the protection of the underlying systems is paramount to the success of the organization. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization as well as the welfare of individuals.[4] Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information. Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for building effective security assessment plans and procedures to enable the assessment of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*, and any additional security controls developed by the organization. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating more cost-effective assessments of security controls contributing to the determination of overall control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support information sharing, security accreditation decisions, and FISMA compliance.

[3] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[4] When selecting security controls for an information system, the organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts.

The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. State, local, and tribal governments, as well as private sector organizations that compose the critical infrastructure of the United States, are also encouraged to consider the use of these guidelines, as appropriate.

Organizations should use this publication in conjunction with an approved system security plan to create a viable security assessment plan for producing and compiling the information necessary to determine the effectiveness of the security controls employed within the information system. The assessment procedures from NIST Special Publication 800-53A should be used as a starting point for and as input to the security assessment. In developing an effective security assessment plan, organizations should tailor and supplement the procedures contained in this publication as needed, taking into consideration existing information about the security controls such as the results from organizational assessments of risk, any platform-specific dependencies in the deployed hardware, software, or firmware, and any assessment procedures needed as a result of organization-specific controls not included in NIST Special Publication 800-53.[5] The selection of appropriate assessment procedures for a particular information system depends on three factors:

- The security categorization of the information system in accordance with FIPS 199 and NIST Special Publication 800-60;
- The security controls from NIST Special Publication 800-53 and any organization-specific controls selected and employed to protect the information system;[6] and
- The level of assurance that the organization must have in determining the effectiveness of the security controls in the information system.

The extent of security control assessments should always be risk-driven, taking advantage of the flexibility in NIST Special Publication 800-53A and applying the results of risk assessments in determining the most cost-effective implementation of this key element in the organization's information security program. The use of NIST Special Publication 800-53A as a starting point in the process of defining procedures for assessing the security controls in an organizational information system, promotes a more consistent level of security within the organization and offers the needed flexibility to customize the assessment based on specific organizational policies and requirements, known threat and vulnerability information, operational considerations, information system and platform dependencies, and tolerance for risk.[7] Ultimately, organizations must balance the cost of implementing a sufficiently strong set of security controls for an information system that adequately protects the organization's operations and assets and the cost of assessing those controls to help determine overall control effectiveness. Based on the above considerations, organizations make the final determination on the extent of security assessments to include the level of effort and resources expended during those assessments.

[5] For example, detailed test scripts may need to be developed for the specific operating system, network component, middleware, or application employed within the information system to adequately assess certain characteristics of a particular security control. Such test scripts are at a lower level of detail than provided by the assessment procedures contained in Appendix F (Assessment Procedures Catalog) and are therefore, beyond the scope of this publication.

[6] The set of agreed-upon security controls for the information system are documented in the system security plan after the initial selection and supplementation of the controls as described in NIST Special Publication 800-53. The security plan is approved by appropriate organizational officials prior to the start of the security assessment.

[7] In this publication, the term *risk* is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation) and assets, to individuals, to other organizations, and to the nation.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of information system and information security professionals including:

- Individuals with information system and security management and oversight responsibilities (e.g., authorizing officials, senior agency information security officers, information security managers);
- Individuals with information system development and integration responsibilities (e.g., product developers, program managers, systems integrators);
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, mission/information owners, and information system security officers); and
- Individuals with information system and security assessment and monitoring responsibilities (e.g., system evaluators, certification agents/teams, independent verification and validation assessors, auditors, inspectors general, information system owners).

1.3 SYSTEM DEVELOPMENT LIFE CYCLE

Security assessments can be effectively carried out at various stages in the system development life cycle[8] to increase the grounds for confidence or assurance that the security controls employed with an information system are effective in their application. This publication provides a comprehensive set of assessment procedures to draw upon for supporting security assessment activities during the system development life cycle. For example, security assessments can be conducted by information system developers and by system integrators during the system development and acquisition phase of the life cycle to help ensure that the security controls required for the protection of the system are properly designed, developed, and implemented.[9] This assessment process is often referred to as developmental security testing and evaluation (ST&E). The assessment procedures described in Appendix F can assist in developing ST&E procedures that can be employed during the initial stages of the system development life cycle. Security assessments can also be conducted by information system owners, security officers, independent certification agents, auditors, and inspectors general during the operations and maintenance phase of the life cycle to help ensure that the security controls are effective in the operational environment where the system is deployed.[10] Finally, at the end of the life cycle, security assessments can be conducted as part of ensuring, for example, that important organizational information is purged from the information system prior to disposal.

[8] There are typically five phases in the system development life cycle: (i) system initiation; (ii) system development and acquisition; (iii) system implementation; (iv) system operations and maintenance; and (v) system disposal. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.

[9] Security assessments can also be conducted by the developers of commercial off-the-shelf information technology component products that are to be used in organizational information systems. These types of assessments can be conducted either by the product developer during the development process or by independent, third-party testing laboratories after the development process has been completed.

[10] Security assessors using the assessment procedures from NIST Special Publication 800-53A should work closely with information system owners and authorizing officials to ensure that the procedures selected for the assessment are appropriate for the information system being assessed. Application of the assessment procedures without careful consideration of the particular information system and its operational environment may be detrimental to the overall assessment process and produce misleading results.

1.4 ENTERPRISE-WIDE STRATEGY FOR SECURITY ASSESSMENTS

Organizations are encouraged to develop an enterprise-wide strategy for security assessments to facilitate a more cost-effective and consistent implementation of assessment processes and to take advantage of the sharing of assessment results. This enterprise-wide strategy should begin by applying the initial components of the NIST Risk Management Framework (RMF)[11] to all information systems within the organization, with an organizational view of the security categorization process, the security control selection process, and the identification of common security controls. Maximizing the number of common controls employed within an organization: (i) significantly reduces the cost of development, implementation, and assessment of security controls; (ii) allows organizations to centralize the security control assessments and to amortize the cost of those assessments across the entire enterprise; and (iii) increases overall security control consistency. An aggressive, enterprise-wide approach to identifying common controls early in the RMF process facilitates a more global strategy for assessing those controls and sharing essential assessment results with information system owners. The sharing of assessment results among key organizational officials across information system boundaries has many important benefits including:

- Providing organizations the capability to review assessment results for all information systems and to make enterprise-wide, mission-oriented decisions on risk mitigation activities according to organizational priorities, organizational assessments of risk, and the impact levels of the information systems supporting the organization;
- Providing organizations a more global view of systemic weaknesses and deficiencies occurring in information systems across the organization; and
- Providing organizations an opportunity to develop enterprise-wide solutions to information security problems and information system owners an opportunity to increase their knowledge base regarding threats, vulnerabilities, and strategies for more cost-effective solutions to common information security problems.

Figure 1 illustrates the relationship among the independent information system assessments and the overall determination and acceptance of enterprise mission risk.

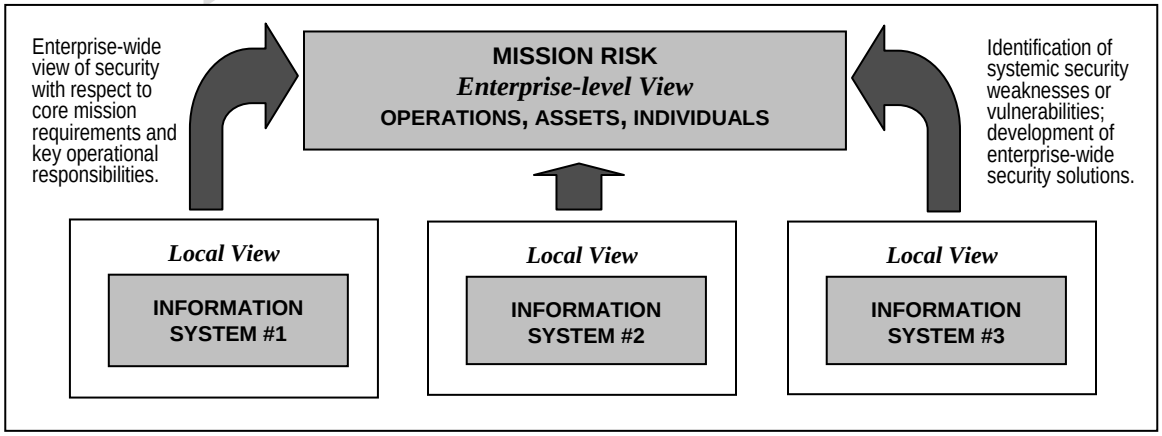

FIGURE 1. INFORMATION SYSTEM ASSESSMENTS AND MISSION RISK

[11] The Risk Management Framework is described in NIST Special Publication 800-53 and consists of an eight-step security life cycle process to ensure the development and implementation of comprehensive information security programs for organizations. Security assessments are addressed in the *assess* and *monitor* steps of the framework. See Appendix J for a summary of the Risk Management Framework.

While the conduct of the security assessment is the primary responsibility of the information system owner[12] with oversight by the authorizing official, there should be significant involvement in the assessment process by other parties within the organization who have a vested interest in the outcome of the assessment. Other interested parties include, for example, mission and information owners (when those roles are filled by someone other than the information system owner) and information security officials. It is imperative that the information system owner coordinate with the other parties in the organization having an interest in the security assessment to ensure that: (i) the organization's core missions and business functions are satisfied and that all risk factors affecting the ability of the enterprise to successfully carryout out those missions and business functions are thoughtfully considered; and (ii) an appropriate degree of objectivity and independence is applied to the security assessment process to avoid conflicts of interest in determining security control effectiveness or the capability of the information system to protect the organization's operations and assets, individuals, other organizations, and the nation.[13]

1.5 RELATIONSHIP TO OTHER ASSESSMENT PROCESSES AND PUBLICATIONS

NIST Special Publication 800-53A has been designed to be used with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. In particular, the assessment procedures contained in this publication and the guidelines provided for developing security assessment plans for organizational information systems directly support the security certification and continuous monitoring phases in the four-phase certification and accreditation process. The primary objective of the security certification phase is to help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). The security assessment procedures defined in this publication provide a foundational level of assessment to support the security certification process. As the information system moves into the continuous monitoring phase (subsequent to system authorization during the security accreditation phase), organizations can select an appropriate subset of the assessment procedures from the security assessment plan based on the assessment procedures defined in this publication to assess the security controls on an ongoing basis. The assessment procedures selected for the follow-on assessments that occur during the continuous monitoring phase are based on the organization's assessment of risk, the plan of action and milestones for the information system, and organizational security policies, any of which may indicate the need for greater emphasis on selected security controls.

Organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available on information system components from independent, third-party testing, evaluation, and validation. Product testing, evaluation, and validation are routinely conducted today on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, web browsers, web applications, smart cards, biometrics devices, personal identity verification devices, web applications, network devices, and hardware platforms using national and international standards. If an information system component product is identified as providing support for the implementation of a particular security control in NIST Special Publication 800-53, then any available evidence produced during the product testing,

[12] The information system owner is the organizational official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

[13] Security controls CA-4(1) and CA-7(1) in NIST Special Publication 800-53 require an independent certification agent or team be employed by the organization when conducting assessments of moderate-impact and high-impact information systems.

evaluation, and validation processes (e.g., security specifications, validation reports, and validation certificates)[14] should be used to the extent that it is applicable. This evidence should be combined with the assessment-related evidence obtained from the application of the assessment procedures in this publication, to cost-effectively produce the information necessary to determine whether the security control is effective or ineffective in its application.

1.6 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control assessments including: (i) the conceptual framework for the development of specific procedures for assessing the security controls in NIST Special Publication 800-53; (ii) a description of the components that compose the assessment framework; and (iii) the process of deriving assessment procedures using the assessment framework.
- **Chapter Three** describes the process of assessing the security controls in organizational information systems including: (i) building an effective assurance case; (ii) the activities needed to prepare for a security assessment; (iii) the development of effective security assessment plans; (iv) the process of analyzing, documenting, and reporting security assessment results; and (v) the importance of continuous monitoring of security controls in the long-term protection strategies for organizations.
- **Supporting appendices** provide more detailed assessment-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a description of assessment methods; (v) assessment expectations for low-impact, moderate-impact, and high-impact information systems; (vi) a master catalog of assessment procedures that can be used to develop plans for assessing the security controls; (vii) penetration testing guidelines; (viii) an assessment procedure selection work sheet; (ix) techniques to manage assessment results and a security assessment reporting form; and (x) a description of the NIST Risk Management Framework.

[14] Organizations should review the component product's available information to determine: (i) what security controls are implemented by the product; (ii) if those security controls meet intended control requirements of the information system under assessment; (iii) if the configuration of the product and the environment in which the product operates are consistent with the environmental and product configuration as stated by the vendor/developer; and (iv) if the assurance requirements stated in the developer/vendor specification satisfies the assurance requirements for assessing those controls. Meeting the above criteria provides a sound rationale that the product is suitable and meets the intended security control requirements of the information system under assessment.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY CONTROL ASSESSMENTS

This chapter describes the basic concepts associated with assessing the security controls in an information system including: (i) the conceptual framework used for developing assessment procedures; (ii) the definitions of individual framework components; and (iii) the process employed to derive assessment procedures for security assessment plans. The information contained in this chapter can be used by organizations: (i) to obtain a better understanding of how the assessment procedures in this document were developed; and (ii) to develop, when necessary, additional assessment procedures that are not contained in the catalog in Appendix F.

2.1 FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES

A conceptual framework is used to describe the process of creating assessment procedures for assessing security controls defined in NIST Special Publication 800-53 and to provide guidelines for organizations and third parties in developing additional assessment procedures, when necessary. There are three top-level components included within the framework: (i) an input component; (ii) a processing component; and (iii) an output component. The input component includes a NIST Special Publication 800-53 unique identifier for the security control or control enhancement that is the subject of the assessment (e.g., CP-1, CP-2 (1)) and the FIPS 199 impact level (i.e., low, moderate, or high) of the information system where the control is employed. The processing component includes a set of assessment objectives, assessment methods, and assessment objects that are associated with the security control and the impact level of the information system. The output component consists of an assessment procedure (i.e., a set of procedural steps) that can be used by assessors to obtain evidence for determining security control effectiveness. Figure 2 illustrates the components of the conceptual framework used to develop assessment procedures for security controls and control enhancements.

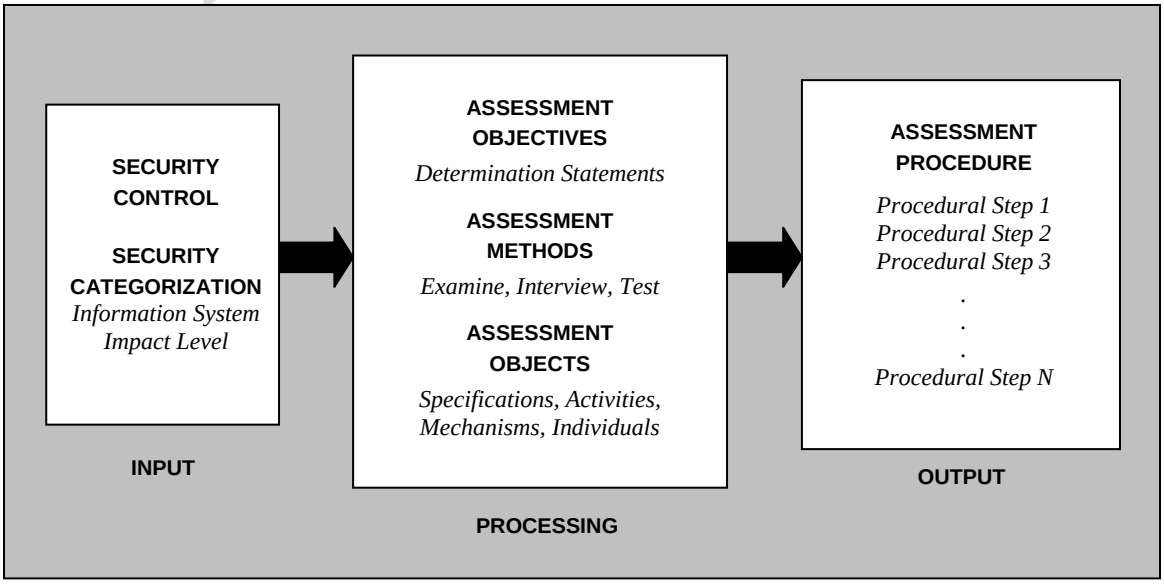

FIGURE 2: CONCEPTUAL FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES

2.2 DEFINING THE FRAMEWORK COMPONENTS

An assessment procedure consists of a set of procedural steps that are created to achieve one or more assessment objectives by applying assessment methods to assessment objects. The assessment objectives defined in the processing component of the framework include a set of *determination statements* related to the particular security control under assessment. The determination statements are closely linked to the content of the security control (i.e., the security control functionality) and the assurance requirements in NIST Special Publication 800-53 to ensure traceability of assessment results back to the fundamental control requirements. The application of an assessment procedure to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the security control.

The assessment objects defined in the processing component of the framework include *specifications*, *mechanisms*, *activities*, and *individuals*. Specifications are the document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. Mechanisms are the specific hardware, software, or firmware safeguards and countermeasures employed within an information system.[15] Activities are the specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above. With regard to the framework, each security control under assessment has a set of assessment objects that are applicable to the control.

The assessment methods defined in the processing component of the framework include *examine*, *interview*, and *test*. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The primary purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence. The *interview* method is the process of conducting discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

Each of the assessment methods described above has a set of associated attributes which help define the expected level of effort, or work factor, for the assessment. The two attributes employed within the conceptual framework are *depth* and *coverage*. The depth attribute addresses the rigor of and level of detail in the examination, interview, and testing processes. Values for the depth attribute include generalized, focused, and detailed. The coverage attribute addresses the scope or breadth of the examination, interview, and testing processes including the number and type of specifications, mechanisms, and activities to be examined or tested and the number and types of individuals to be interviewed. Values for the coverage attribute include representative, specific, and comprehensive. Appendix D provides attribute definitions and descriptions of each assessment method.

[15] Mechanisms also include physical protection devices associated with an information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes, etc.).

The selection of appropriate values for the depth and coverage attributes associated with a particular assessment method is based on the information system impact level where the security control under assessment is employed and is derived from the assurance requirements defined in NIST Special Publication 800-53. These assurance requirements are levied on security control developers and implementers.[16] Based on the assurance requirements, control developers and implementers execute required activities and thereby, as an inherent part of developing or implementing the control, produce the necessary control documentation, conduct essential analyses, and define actions that must be performed during control operation. The purpose of these activities is to provide increased grounds for confidence that the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessors subsequently use the information resulting from these developer and implementer activities during the assessment process to develop the requisite evidence used in determining if security controls are effective in their application.[17]

A set of assessment expectations for low-impact, moderate-impact, and high-impact information systems for a range of assessment objects including specifications, mechanisms, and activities is provided in Appendix E. These assessment expectations are derived from the assurance requirements in NIST Special Publication 800-53 and provide assessors with important reference points as to what findings obtained from the application of the assessment procedures are acceptable for subsequent use by the organization in determining security control effectiveness. Table 1 provides a summary of the assessment expectations by information system impact level.

TABLE 1: ASSESSMENT EXPECTATIONS BY INFORMATION SYSTEM IMPACT LEVEL

ASSESSMENT EXPECTATIONS	INFORMATION SYSTEM IMPACT LEVEL		
	LOW	MODERATE	HIGH
Security controls are in place with no obvious errors.	√	√	√
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	---	√	√
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	---	---	√
Grounds for a high degree of confidence that the security controls are complete, consistent, and correct. ***Beyond minimum recommendations of NIST Special Publication 800-53A***	*For environments with specific and credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets.*		

[16] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls within an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

[17] For example, the assurance requirements in NIST Special Publication 800-53 at the moderate-impact level are designed to ensure that security controls within the information system contain specific actions and the assignment of responsibilities to provide increased grounds for confidence that the controls are implemented correctly and operating as intended. At the high-impact level, the assurance requirements are designed to ensure that when security controls are implemented, the controls will continuously and consistently (i.e., across the information system) meet their required function or purpose and support improvement in the effectiveness of the controls. These requirements are reflected in the associated security control assessment procedures at the appropriate impact level of the information system under assessment.

2.3 DERIVING ASSESSMENT PROCEDURES

With respect to the components defined in the above framework, the derivation of assessment procedures proceeds by using the unique identifier for the security control, parsing the text of the control into assessable components, and incorporating supplemental guidance, as appropriate. There are two types of assessment procedures defined in this publication and used during the assessment of security controls: (i) a *specialized assessment procedure*; and (ii) an *extended assessment procedure*. A specialized assessment procedure is unique to an individual security control or control enhancement. Specialized assessment procedures reflect the NIST Special Publication 800-53 requirement for assurance that the specified functionality within a security control or control enhancement has been implemented. The extended assessment procedure, which complements the specialized assessment procedures, reflects other aspects of the Special Publication 800-53 assurance requirements such as the requirement for assigned responsibilities and specific actions supporting increased grounds for confidence that when the security control is implemented, it will meet its required function or purpose. Organizations have discretion on how the extended assessment procedure is applied during an assessment. The extended assessment procedure can be applied to individual security controls or to a group of security controls (e.g., the set of security controls in a particular security control family or to the entire set of controls in an assessment). Specialized and extended assessment procedures are used in conjunction with one another in obtaining the necessary assessment results. The example below illustrates how specialized assessment procedures are derived and how the extended assessment procedure can be applied in support of the specialized assessment procedures.

Deriving a specialized assessment procedure for a security control

Consider security control CP-1:

> **CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES**
>
> Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
>
> Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

The assessment objectives associated with the security control are identified first. The control statement defines what is expected to be achieved by applying the control within the information system and forms the basis for defining the assessment objectives using appropriate determination statements. In this example, there are several required actions defined in the security control including developing, documenting, disseminating, and updating a contingency planning policy. In addition, the control requires the contingency planning policy to address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Finally, the control requires developing, documenting, disseminating, and updating procedures for implementing the contingency planning policy and for achieving policy-compliant implementations of each of the associated contingency planning controls.

Given the above requirements, an initial assessment objective for security control CP-1 can be expressed as follows:

ASSESSMENT OBJECTIVE:

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

A second assessment objective, further addressing the more detailed aspects of security control CP-1 can be expressed as follows:

ASSESSMENT OBJECTIVE:

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Each of the determination statements in the assessment objectives described above, is either traceable to requirements in the base security control or the supplemental guidance in NIST Special Publication 800-53. This ensures that all aspects of the security control are assessed and that any weaknesses or deficiencies in the control can be identified and remediation actions taken.

After the assessment objectives are established, the appropriate assessment objects are determined. In this example, the security control addresses both policy and procedures that, using the definitions for assessment objects, are considered *specifications*. Thus, the assessment objects for the security control are policy specifications and procedure specifications. Finally, the assessment methods to be used in assessing the objects are identified.[18] In accordance with the assessment method descriptions in Appendix D, the *examine* method is used to make assessments based upon specifications. The assessment method attribute values for depth and coverage are also identified to indicate the rigor and intensity to be applied in examining the assessment objects. Therefore, the application of the assessment method to assessment objects can be expressed as follows:

ASSESSMENT METHODS AND OBJECTS:

Examine (DEPTH = **X**, COVERAGE = **Y**): Contingency planning policy, procedures, related documents or records;

Where: For low-impact systems, the values for **X** and **Y** are **generalized** and **representative**, respectively;
For moderate-impact systems, the values for **X** and **Y** are **focused** and **specific**, respectively; and
For high-impact systems, the values for **X** and **Y** are **detailed** and **comprehensive**, respectively.

[18] Whereas the assessment methods that should be used have been included in the catalog of assessment procedures in Appendix F, these are not necessarily intended to be exclusive and, depending on the particular circumstances of the information system to be assessed, other assessment methods may also be used.

As indicated above, the values for the depth and coverage attributes associated with the assessment methods reflect the impact level of the information system where the security controls are employed and assessed. Thus, the expected level of effort expended by assessors in assessing a particular security control (i.e., the extent, rigor, and intensity of the assessor's activities) will vary based upon the values assigned to the depth and coverage attributes. Appendix E provides more detailed information on assessment expectations and the values for depth and coverage attributes for each information system impact level. Using the components of the framework, a complete assessment procedure for security control CP-1 can be formulated. In this example, there are two procedural steps that compose the assessment procedure. The first step, denoted CP-1.1, is expressed as follows:

CP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents contingency planning policy and procedures;* *(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and* *(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities. * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.

The second step, denoted CP-1.2, is expressed as follows:

CP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and* *(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities. * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.

A similar procedural step is produced for every assessment objective within an assessment procedure defined for the security control under assessment. The steps within a particular assessment procedure are numbered sequentially (e.g., CP-1.1, CP-1.2 ,…, CP-1.n). If the security control has any enhancements, procedural steps are developed for each enhancement using the same process as for the base control. The resulting steps within the assessment procedure are numbered sequentially (e.g., CP-2(1).1 indicating the first step for the first enhancement for security control CP-2).[19]

Applying the extended assessment procedure

In addition to the specialized assessment procedures that are applied to individual security controls as in the CP-1 example above, an extended assessment procedure is applied to the assessment as a whole. The extended assessment procedure is designed to work with and complement the specialized assessment procedures listed in Appendix F to produce additional evidence contributing to the grounds for confidence in the effectiveness of the security controls employed in the information system. The extended assessment procedure and the associated procedural steps are also linked closely to the impact level of the information system and the assurance requirements in NIST Special Publication 800-53. Consider the NIST Special Publication 800-53 assurance requirements for low-impact systems:

Assurance Requirement: **The security control is in effect and meets explicitly identified functional requirements in the control statement.**

Supplemental Guidance: For security controls in low impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

The basic assurance requirement for low-impact systems is covered by the specialized assessment procedure for the control. However, an additional assurance requirement is identified in the supplemental guidance and addressed in the extended assessment procedure. Specifically, for a low-impact information system, the following procedural step, EAP.1, from the extended assessment procedure is applied:

EAP.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization has a process in place to address in a timely manner, any flaws discovered in the implementation or application of the security controls in the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Policies, procedures, records, documents, activities, or mechanisms related to addressing flaws in security controls or control enhancements.

[19] NIST Special Publication 800-53A provides flexibility to organizations in deciding how many assessment objectives to define for each security control and how to capture the individual control requirements among assessment objectives. In the CP-1 example above, the control requirements are divided among two assessment objectives primarily because the elements within the security control are of two types—actions (first objective) and adequacy (second objective). However, an assessment procedure consisting of one objective covering all control requirements would also be acceptable if the organization chose to organize its procedure in that manner. In deciding how many assessment objectives to define, it is recommended that the number of objectives be kept as small as possible while still providing a meaningful subdivision of assessment results and providing for any needed differentiation between objectives and assessment methods that apply.

The extended assessment procedure applies to the entire assessment, yet may be implemented control by control, by group of controls, or collectively across all controls in the information system simultaneously. In this situation, the organization, based on the information system security plan for implementing the NIST Special Publication 800-53 assurance requirements, may have decided to have a process in place to address flaws at the individual security control level (e.g., CP-1) or may have decided to rely on a single process to document and address flaws at the security control family level (e.g., Contingency Planning family). Extending that concept further, the organization may have also decided to employ an enterprise-wide process to document flaws in the security controls across the entire information system. Whether the organization chooses to implement one process or many processes will determine how the assessor applies the extended assessment procedure. The specific application of the extended assessment procedure should be described in the security assessment plan. Additional procedural steps from the extended assessment procedure are included in the assessment as the impact level of the information system increases. See Appendix F for the complete extended assessment procedure.

The preceding discussion illustrates the process of how both specialized and extended assessment procedures are derived from the conceptual framework using the security controls and the assurance requirements in NIST Special Publication 800-53. The framework helps to ensure that the procedures used to assess the security controls defined in Special Publication 800-53 are consistent when applied to multiple information systems across the organization. Ultimately, the assessment procedures become part of a catalog of procedures in Appendix F, which documents and organizes the procedures according to the seventeen families of security controls defined in Special Publication 800-53. Organizations can use the assessment procedures in Appendix F as a starting point for developing comprehensive organization/system-specific assessment procedures for security assessment plans to support a variety of potential assessment activities associated with obtaining the information necessary for determining the effectiveness of security controls in organizational information systems.

CHAPTER THREE

THE PROCESS

CONDUCTING EFFECTIVE SECURITY ASSESSMENTS

This chapter describes the process of assessing the security controls in organizational information systems including: (i) considerations for building an effective assurance case; (ii) preparing for security assessments; (iii) developing security assessment plans; (iv) approaches for analyzing, documenting, and reporting assessment results; and (v) the importance of continuous monitoring of security controls.

3.1 BUILDING AN EFFECTIVE ASSURANCE CASE

Building an effective assurance case for security control effectiveness is a process that involves: (i) compiling evidence that the controls employed in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system; and (ii) presenting this evidence in a manner that decision makers are able to use effectively in making credible, risk-based decisions about the operation or use of the system. The evidence described above comes from both the implementation of the security controls in the information system and from the assessments of that implementation. Ideally, the assessor is adding to an existing assurance case that started with the specification of the organization's information security needs and was further developed during the design, development, and implementation of the information system.

Assessors obtain the evidence needed during the assessment process to allow the appropriate organizational officials to make objective determinations about the effectiveness of the security controls and the security of the information system. The assessment evidence needed to make such determinations can be obtained from a variety of sources including, but not limited to, information technology product and system assessments. Product assessments (also known as product testing and evaluation) are typically conducted by independent, third-party testing organizations and examine the security functions of products and established configuration settings. Assessments can be conducted against industry, national, and international information security standards as well as developer and vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in millions of information systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the particular products.

System assessments are typically conducted by information systems developers, systems integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs of organizations. These assessors or assessment teams bring together available information about the information system such as the results from product-level assessments, if available, and conduct additional system-level assessments using a variety of methods and techniques. System assessments are used to compile and evaluate the evidence needed by organizational officials to determine how effective the security controls employed in the information system are likely to be in mitigating risks to organizational operations and assets, to individuals, to other organizations, and to the nation. The results from assessments conducted using information system-specific and organization-specific assessment procedures derived from the guidelines in NIST Special Publication 800-53A contribute to compiling the necessary evidence to determine security control effectiveness in accordance with stated assurance requirements in NIST Special Publication 800-53.

In addition to the above assessment-related activities, building effective assurance cases involves other activities carried out by the organization during the security assessment process. Figure 3 provides an overview of the security assessment process that is described in the following sections and employed to determine security control effectiveness.

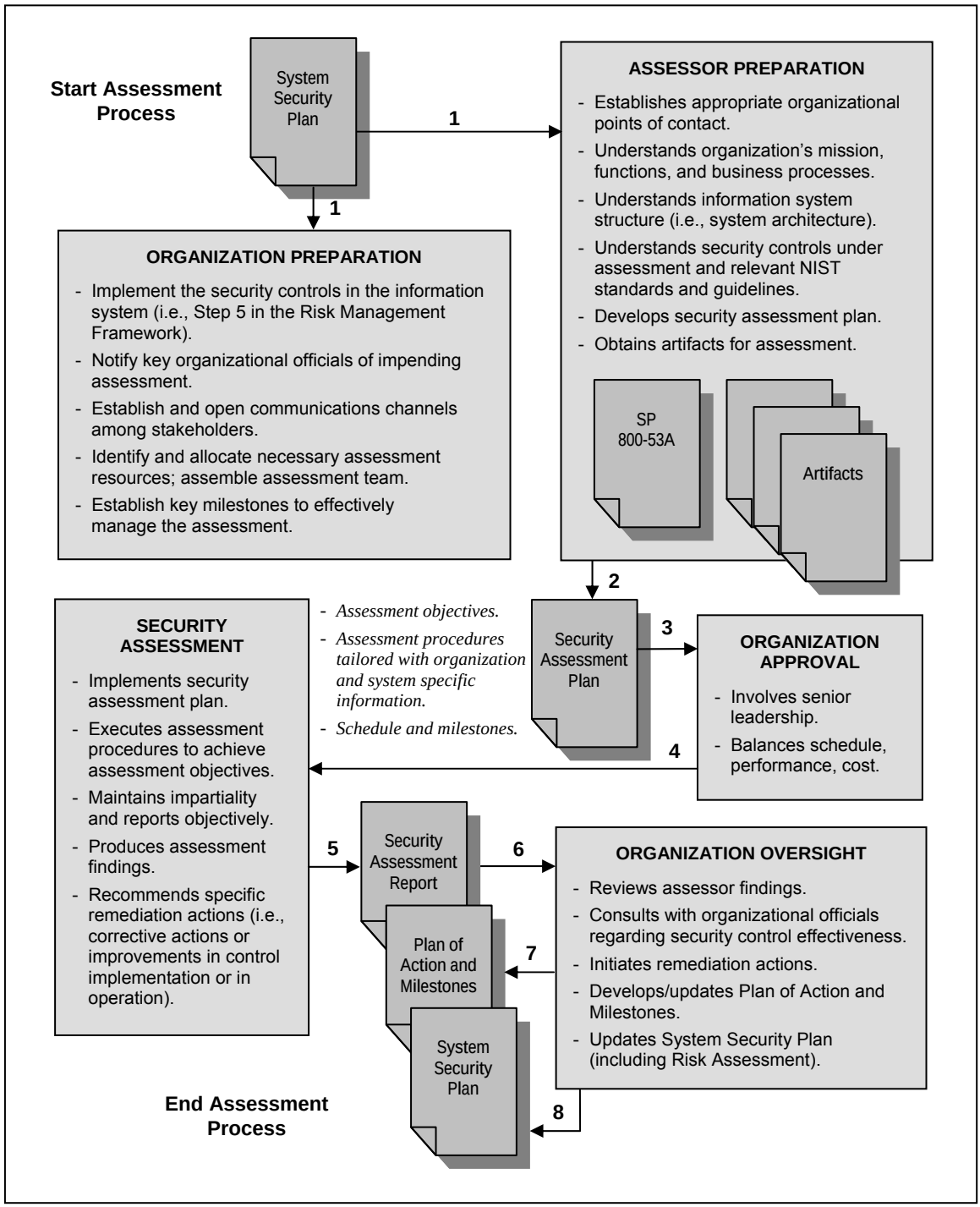

FIGURE 3: SECURITY ASSESSMENT PROCESS OVERVIEW

3.2 PREPARING FOR SECURITY ASSESSMENTS

Conducting security assessments in today's complex environment of sophisticated information technology infrastructures and high-visibility, mission-critical applications can be difficult, challenging, and resource-intensive. However, the stakes have never been higher with regard to knowing whether the security controls employed in federal information systems are effective in their application and adequately protecting critical missions and business functions. Success requires the cooperation and collaboration among all parties having a vested interest in the organization's information security posture, including information system owners, authorizing officials, chief information officers, senior agency information security officers, chief executive officers/heads of agencies, inspectors general, and the OMB. Establishing an appropriate set of expectations before, during, and after the security assessment is paramount to achieving a good outcome—that is, the assessment producing the information necessary for the authorizing official to make a credible, risk-based decision on whether to place the information system into operation or continue its operation. This decision depends largely on the credibility of the information compiled during the security assessment which contributes to understanding the residual risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation.

Thorough preparation by the organization and the assessors and/or assessment teams is an important aspect of conducting effective security assessments. Preparatory activities should address a range of issues relating to the cost, schedule, and performance of the security assessment. From the organizational perspective, preparing for a security assessment includes the following key activities:

- Ensuring that appropriate policies covering security assessments are in place and understood by all organizational elements;
- Ensuring that all steps in the NIST Risk Management Framework prior to the security control assessment step, have been successfully completed and have received appropriate management oversight;
- Establishing appropriate communication channels among organizational officials having an interest in the security assessment; [20]
- Establishing the objective and scope of the security assessment (i.e., the purpose of the assessment and what is being assessed and to achieve the objective);
- Notifying key organizational officials of the impending security assessment and allocating necessary resources to carry out the security assessment;
- Establishing time frames for completing the security assessment and key milestone decision points required by the organization to effectively manage the assessment;
- Identifying and selecting a competent assessor/assessment team that will be responsible for conducting the security assessment, considering issues of assessor independence; and
- Establishing a mechanism between the organization and the assessor and/or assessment team to minimize ambiguities or misunderstandings about security control implementation or security control weaknesses/deficiencies identified during the assessment.

[20] Typically, these individuals include authorizing officials, information system owners, mission and information owners (if other than the information system owner), chief information officers, senior agency information security officers, inspectors general, information system security officers, users and organizations that the information system supports, and assessors (e.g., certification agents/teams, independent auditors).

In addition to the planning activities the organization carries out in preparation for the security assessment, assessors/assessment teams should begin preparing for the security assessment by:

- Obtaining a general understanding of the organization's operations (including mission, functions, and business processes) and how the information system under assessment supports those organizational operations;
- Obtaining an understanding of the structure of the information system (i.e., system architecture) that is the subject of the security assessment;
- Obtaining a thorough understanding of the security controls being assessed together with appropriate FIPS and NIST Special Publications that are referenced in those controls;
- Establishing appropriate organizational points of contact needed to carry out the security assessment;
- Obtaining artifacts needed for the security assessment (e.g., policies, procedures, specifications, designs, records, administrator/operator manuals, information system documentation, previous assessment results); and
- Developing a security assessment plan.

Security control assessors are responsible for obtaining the evidence necessary for determining the effectiveness of the security controls in the organization's information system. Assessors are *not* responsible for determining if the organization has selected the appropriate set of security controls to achieve *adequate security* in protecting organizational operations, organizational assets, individuals, other organizations, and the nation. The selection of an appropriate set of security controls for an information system is the responsibility of the information system owner, mission and information owners (if those positions are held by individuals other than the information system owner), and other designated organizational officials (e.g., chief information officer, senior agency information security officer, and authorizing official). Security control selection should be accomplished in accordance with the organization's assessment of risk and the guidelines set forth in NIST Special Publication 800-53 for tailoring and supplementing the baseline set of security controls for the information system. The determination that the correct set of security controls has been selected is made as part of the system security plan approval process which takes place before the security assessment.

Security control assessors should review the system security plan to ascertain whether or not the plan addresses all of the security controls selected for implementation during the baseline tailoring and supplementation process. Should assessors find any apparent discrepancies in the security plan with regard to meeting the minimum security requirements defined in FIPS 200 or following the security control selection process established in NIST Special Publication 800-53, they should report such deficiencies to appropriate organizational officials with a recommendation that the plan be amended to remedy the deficiencies. If the security plan is not appropriately amended, assessors should include in their findings, the details of such deficiencies along with any potential compromises to confidentiality, integrity, and availability within the information system that may result.

In preparation for the assessment of security controls, the necessary background information should be assembled and made available to the assessors or assessment team. The organization should identify and arrange access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating all security policies and associated procedures for implementing policy-compliant controls; (ii) the security policies for the information system and any associated implementing procedures; (iii) individuals or groups

responsible for the development, implementation, operation, and maintenance of security controls; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after-action reports, agreements, accreditation packages) associated with the implementation and operation of security controls; and (v) the objects to be assessed. The availability of essential documentation as well as access to key organizational personnel and the information system being assessed are paramount to a successful assessment of the security controls.

3.3 DEVELOPING SECURITY ASSESSMENT PLANS

The *security assessment plan* provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. The output and end result of the security assessment is the *security assessment report*, which documents the assurance case for the information system and is one of three key documents in the security accreditation package developed by information system owners for authorizing officials.[21] The security assessment report includes information from the assessor (in the form of assessment findings) necessary to determine the effectiveness of the security controls employed in the information system and the organization's overall effectiveness determination based upon the assessor's findings. The security assessment report is a key factor in the authorizing official's determination of risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Appendix I provides additional information on the format and content of security assessment reports.

There are a series of distinct steps that assessors should consider in developing a plan to assess the security controls in an information system. These steps include: (i) determining the type of security assessment and which security controls and control enhancements are to be included in the assessment; (ii) selecting the appropriate assessment procedures to be used during the security assessment; (iii) tailoring the selected assessment procedures for the information system impact level and organization's operating environment; (iv) developing additional assessment procedures, if necessary, to address security controls and control enhancements that are not contained in NIST Special Publication 800-53 or to address additional assurance needs beyond what is provided in NIST Special Publication 800-53A; (v) optimizing the assessment procedures to reduce duplication of effort and provide cost-effective assessment solutions; (vi) developing a strategy to apply the extended assessment procedure; and (vii) finalizing the assessment plan and obtaining the necessary approvals to execute the plan.

Determine which security controls are to be assessed—

The security plan for the information system undergoing assessment provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The assessor starts with the security controls described in the security plan and considers the purpose of the assessment. A security assessment can be a *complete* assessment of all security controls in the information system (e.g., the certification phase of the certification and accreditation process) or a *partial* assessment of the security controls in the information system (e.g., the continuous monitoring phase of the certification and accreditation process where subsets of the controls in the information system are assessed on an ongoing basis). For partial assessments, the information system owner collaborates with organizational officials having an interest in the assessment (e.g., chief information security officer, senior agency information security officer, mission/information owners, and authorizing

[21] In accordance with NIST Special Publication 800-37, the security accreditation package consists of the security plan (including the risk assessment), the security assessment report, and the POAM.

official) to determine which security controls from the system security plan are to be assessed during the assessment. Selection of the security controls depends on the continuous monitoring schedule established by the information system owner to ensure that all controls are assessed during the three-year accreditation cycle, that items on the plan of action and milestones receive adequate oversight, and that controls with greater volatility are assessed more frequently.[22]

Select the appropriate procedures to assess the security controls—

NIST Special Publication 800-53A, Appendix F, provides a specialized assessment procedure for each security control and control enhancement in NIST Special Publication 800-53. For each security control and control enhancement in the system security plan to be assessed during the assessment, assessors select the corresponding specialized assessment procedure from Appendix F. The set of selected assessment procedures varies from assessment to assessment based on the current content of the system security plan and on the organization's assessment requirements (e.g., security certification, continuous monitoring). Appendix H provides a work sheet for selecting appropriate specialized assessment procedures for the assessment based on the approved security plan and the particular assessment focus.

Tailor the assessment procedures for specific operating environments—

In a similar manner to how the security controls from NIST Special Publication 800-53 are tailored for the organization's mission, business functions, specifics of the information system, and operating environment, the assessment procedures from Appendix F of this publication are tailored to meet specific organizational needs. Assessment procedures can be tailored: (i) by carefully selecting the assessment objects needed to make appropriate determinations and satisfy assessment objectives; (ii) by assigning depth and coverage attribute values in accordance with the assigned information system impact level; (iii) by eliminating assessment procedures for common security controls if those controls have been assessed by another documented assessment process; (iv) by developing information system/platform-specific and organization-specific extensions to provide the level of detail necessary to successfully carry out the assessment of the security controls; (v) by incorporating assessment results from previous assessments where the results demonstrate a sufficient coverage; (vi) by reducing the assessment requirements on low-impact and moderate-impact information systems by allowing optional use of selected determination statements and assessment methods; and (vii) by developing extensions and making appropriate adjustments in assessment procedures to be able to obtain the requisite assessment evidence from external providers.

Assessment object-related considerations—

Recognizing that organizations can specify, organize, document, and configure their information systems in a variety of ways, the assessment objects identified in Appendix F that are used in conjunction with the interview, examine, and test methods should be considered suggested objects where information/evidence may be found. As such, assessors are expected to use their judgment in applying the designated assessment methods to the associated set of assessment objects. Each assessment method listed in a procedural step should be applied to a sufficient number of assessment objects to produce the information necessary to make the determination in the determination statement and to satisfy the assessment objective. It may not always be necessary to apply each assessment method to every assessment object in the list.

[22] Section 3.5 provides further information on selecting security controls in an information system to be assessed as part of a continuous monitoring process. In addition, NIST Special Publication 800-37 provides guidance on continuous monitoring as part of the security certification and accreditation process.

Depth- and coverage-related considerations—

Each assessment method used in an assessment procedure contains depth and coverage attributes that are described in Appendix D and are directly linked to the impact level of the information system containing the security controls under assessment as indicated in Appendix E. The attribute values are assigned based on information system impact level and affect the extent, rigor, and intensity of the assessment procedure executed by the assessor. For example, for low-impact information systems, the attribute values assigned to the depth and coverage attributes respectively, are *generalized* and *representative*. This means that as assessors carry out the specialized assessment procedures for the security controls and control enhancements in the security plan including conducting interviews with individuals, examining policies, procedures, and other documentation, and testing portions of the information system, the work factor is guided by the definitions in Appendix D for generalized depth and representative coverage.

Common security control-related considerations—

Assessors should note which security controls (or parts of controls) in the information system security plan are designated as *common controls*. Since the assessment of common controls is the responsibility of the organizational entity that developed and implemented the controls, the assessment procedures in Appendix F used to assess these controls should incorporate assessment results from that organizational entity. Common controls may have been previously assessed as part of the organization's enterprise-wide information security program, or there may be a separate plan to assess the common controls.[23] In either situation, the information system owner coordinates the assessment of all security controls in the information system with appropriate organizational officials (e.g., chief information officer, senior agency information security officer, mission/ information owners, authorizing official) obtaining the results of common control assessments or (if the common controls have not been assessed or are due to be reassessed) making the necessary arrangements to include the common control assessment results in the current assessment.[24]

Another consideration in assessing common security controls is that there are occasionally system-specific aspects of a common control that are not covered by the organizational entities responsible for the common aspects of the control. These types of security controls are referred to as *hybrid controls*. For example, CP-2, the contingency planning security control, may be deemed a hybrid control by the organization since there is a master contingency plan developed by the enterprise for all organizational information systems. However, information system owners are expected to adjust or tailor the contingency plan as necessary, when there are system-specific aspects of the plan that need to be defined for the particular information system where the control is employed. For each hybrid security control, assessors should include in the assessment plan, the portions of the assessment procedures from Appendix F related to the parts of the control that are system-specific to ensure that, along with the results from common control assessments, all aspects of the security control are assessed.

[23] If common control assessment results for moderate-impact and high-impact information systems are to be used for certification activities, then an independent assessment (or independent validation of assessment results) must be conducted and the authorizing official has the right to determine the acceptable degree of assessor independence.

[24] If assessment results are not currently available for the common controls, the assessment plans for the information systems under assessment that depend on those controls should be duly noted. The assessments cannot be considered complete until the assessment results for the common controls are made available to information system owners. NIST Special Publications 800-37 and 800-53 provide guidance on the employment and use of common security controls in organizational information systems.

System/platform and organization-related considerations—

The assessment procedures in NIST Special Publication 800-53A may be extended or adapted to address system/platform-specific or organization-specific dependencies. This situation arises frequently in the assessment procedures associated with the security controls from the technical families in NIST Special Publication 800-53 (i.e., access control, audit and accountability, identification and authentication, system and communications protection). For example, an extension to the IA-2 control for identification and authentication of users might include an explicit examination of the *.rhosts* file for UNIX systems since improper entries in that file can result in bypassing user authentication. Recent test results may also be applicable to the current assessment if those test methods provide a high degree of transparency (e.g., what was tested, when was it tested, how was it tested). Standards-based testing protocols such as Security Content Automation Protocol (SCAP) provide this level of transparency. Further, SCAP checklists and test procedures are organized by NIST Special Publication 800-53 controls to enable efficiency in assessing federal information systems. Additional details on the ISAP/SCAP initiative can be found at the NIST website at http://nvd.nist.gov.

Reuse of assessment evidence-related considerations—

In general, assessors should take advantage of existing security assessment information to facilitate more cost-effective assessments. The reuse of assessment results from previously accepted or approved assessments of the information system should be considered in developing the evidence for determining overall security control effectiveness.[25] The assessment procedures presented in Appendix F are designed to gather or compile evidence for determining if security controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements of the information system. When considering the reuse of assessment results from previous assessments, assessors should validate the credibility of the evidence obtained, the appropriateness of previous analysis, and the applicability of the evidence to present information system operating conditions.[26] It may be necessary, in certain situations, to supplement the previous assessment results under consideration for reuse with additional assessment activities to fully address the assessment objectives. For example, if an independent, third-party evaluation of an information technology product did not test a particular configuration setting that is used by the organization to help protect the information system, then the assessor may need to supplement the original test results with additional testing to cover that configuration setting (i.e., assessment objective) for the current information system environment. The following items should be considered in validating previous assessment results for reuse in the current assessment:

- *Changing conditions associated with security controls over time.*

  Security controls that were deemed effective during previous assessments may have become ineffective due to changing conditions within the information system or the surrounding environment. Thus, assessment results that were found to be previously acceptable may no longer provide credible evidence for determination of security control effectiveness, and a reassessment would be required. Applying previous assessment results to a current assessment requires the identification of any changes that have occurred since the previous

[25] Previously accepted or approved assessments include those assessments of common security controls that are managed by the organization and support multiple information systems.

[26] It should be noted that information technology product assessments are based upon the assumption that the products are properly and appropriately configured when installed in particular information systems in specific operational environments. If not properly configured, the products may not perform in the manner verified during the assessment.

assessment and the impact of these changes on the previous assessment results. For example, reusing previous assessment results that involved examining an organization's security policies and procedures may be acceptable if it is determined that there have not been any significant changes to the identified policies and procedures. Reusing evidence and security control assessment results produced during the initial certification and accreditation of an information system will likely be a cost-effective method for supporting continuous monitoring activities and annual FISMA reporting when the related controls have not changed and there are adequate reasons for confidence in their continued application.

- *The acceptability of using previous assessments.*

  The acceptability of using previous assessment results in a security assessment should be coordinated with and approved by the users of the assessment results. It is essential that the information system owner collaborates with appropriate organizational officials (e.g., chief information officer, senior agency information security officer, mission/information owners, authorizing official) in determining the acceptability of using previous assessment results. The decision to reuse assessment results should be documented in the security assessment plan and the final security assessment report and should be consistent with federal legislation, policies, directives, standards, and guidelines with respect to the security assessments.

- *The amount of time that has transpired since the previous assessments.*

  In general, as the time period between current and previous assessments increases, the credibility/utility of the previous assessment results decreases. This is primarily due to the fact that the information system or the environment in which the information system operates is more likely to change with the passage of time, possibly invalidating the original conditions or assumptions on which the previous assessment was based.

- *The degree of independence of the previous assessments.*

  Assessor independence can be a critical factor in certain types of assessments, especially for information system at the moderate- and high-impact levels. The degree of independence required from assessment to assessment should be consistent. For example, it is not appropriate to reuse results from a previous self-assessment where no assessor independence was required, in a current assessment requiring a greater degree of independence.

Information system impact level-related considerations—

In an effort to apply the appropriate level of effort to the assessment of security controls in organizational information systems in accordance with organizational assessments of risk, a degree of flexibility is provided in the execution of assessment procedures based on the impact level of the information system. Selected determination statements and assessment methods used to conduct assessments of security controls in low-impact and moderate-impact information systems can be optionally employed at the discretion of the organization. The determination statements and assessment methods marked with an "L" or and "M" in the catalog of assessment procedures in Appendix F indicates use of the determination statements or assessment methods is optional for low-impact and moderate-impact information systems, respectively. The decision to reduce the level of effort for the assessment of security controls in low-impact and moderate-impact information systems does not affect the basic requirements in the control as stated in NIST Special Publication 800-53. The decision to employ optional determination statements and assessment methods should be a decision guided by an organizational assessment of risk with input from key organizational officials with a vested interest in the assessment and with responsibility for carrying out or supporting organizational missions and business functions.

External information system-related considerations

The assessment procedures in Appendix F need to be tailored as appropriate to accommodate the assessment of external information systems.[27] Because the organization does not always have direct control over the security controls used in external information systems, or sufficient visibility into the development, implementation, and assessment of those controls, alternative assessment approaches may need to be applied, resulting in the need to tailor the assessment procedures described in Appendix F. Where required assurances of agreed-upon security controls for an information system are documented in contracts or service-level agreements, the assessor should review these contracts or agreements and where appropriate, tailor the assessment procedures to assess either the security controls or the security assessment results provided through these agreements. Additionally, assessors should take into account any assessments that have been conducted, or are in the process of being conducted, for external information systems that are relied upon with regard to protecting the information system under assessment. Applicable information from these assessments, if deemed reliable, should be incorporated into the security assessment report.

Develop assessment procedures for organization-specific security controls—

Based on organizational policies, mission or business function requirements, and an assessment of risk, organizations may choose to develop and implement additional (organization-specific) security controls or control enhancements for their information systems that are beyond the scope of FIPS 200 and NIST Special Publication 800-53. Such security controls are documented in the security plan for the information system as controls not found in Special Publication 800-53. To assess the security controls in this situation, assessors should use the assessment framework described in Chapter Two to develop assessment procedures for those controls and control enhancements. The assessment procedures developed should be integrated into the security assessment plan.

Develop assessment procedures for additional assurance requirements—

The assessment procedures described in NIST Special Publication 800-53A correspond with the minimum assurance requirements identified in NIST Special Publication 800-53. However, when the organization is relying upon security controls to mitigate risks arising from highly skilled, highly motivated, and well-financed threat sources, Special Publication 800-53 requires additional assurances for moderate-impact and high-impact information systems. As indicated in the last row in Table E-1 in Appendix E, the assessment procedures for these added assurances are beyond the scope of the minimum assessment expectations currently described in this document. Therefore, when such additional assurances apply, the organization should develop additional assessment procedures to provide the necessary evidence that the effected security controls have been developed in a manner that supports a high degree of confidence that the controls are complete, consistent, and implemented correctly. Additionally, organizational risk management needs may dictate the development of assessment procedures beyond the procedures provided in this publication. In both cases, the additional security assessment procedures should be integrated into the security assessment plan.

[27] An *external information system* is an information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. NIST Special Publication 800-53 provides additional guidance on external information systems and the effect of employing security controls in those types of environments.

Optimize the selected assessment procedures to ensure maximum efficiency—

Assessment efficiencies and economies of scale may be leveraged by determining which security controls and control families are similar in structure, objective, and intent. Once this analysis is completed, assessors have a great deal of flexibility in organizing a security assessment plan that meets the needs of the organization and that provides the best opportunity for obtaining the necessary evidence to determine security control effectiveness, while reducing overall assessment costs. Combining and consolidating procedural steps is one area where this flexibility can be applied. During the assessment of an information system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of security controls. To save time, reduce assessment costs, and maximize the usefulness of assessment results, assessors should review the selected assessment procedures for the security control families and combine or consolidate procedural steps whenever possible or practicable. For example, assessors may wish to consolidate interviews with key organizational officials dealing with a variety of security-related topics. Assessors may have other opportunities for significant consolidations and cost savings by examining all security policies and procedures from the seventeen families of security controls at the same time or organizing groups of related policies and procedures that would be amenable to a single, unified review. Obtaining and examining configuration settings from similar hardware and software components within the information system is another example that can provide significant assessment efficiencies.

An additional area for consideration in optimizing the assessment process is the sequence in which security controls are assessed. The assessment of some security controls before others may provide information that facilitates understanding and assessment of other controls. For example, security controls such as CM-2 (Baseline Configuration), CM-8 (Information System Component Inventory), PL-2 (System Security Plan), RA-2 (Security Categorization), and RA-3 (Risk Assessment) produce general descriptions of the information system. Assessing these security controls early in the security assessment process may provide a basic understanding of the information system that can aid in assessing other security controls. The supplemental guidance of many security controls also identifies related controls that can provide useful information in organizing the assessment procedures. For example, AC-19 (Access Control for Portable and Mobile Devices) lists security controls MP-4 (Media Storage) and MP-5 (Media Transport) as being related to AC-19. Since AC-19 is related to MP-4 and MP-5, the sequence in which assessments are conducted for AC-19, MP-4, and MP-5 may facilitate the reuse of assessment information from one control in assessing other related controls.

Develop strategy for incorporating the extended assessment procedure—

Organizations have great flexibility in achieving the developer/implementer assurance requirements in NIST Special Publication 800-53. For requirements such as assurance that flaws are addressed in a timely manner, the organization can accomplishment these on a control-by-control basis, on a by-type-of-control basis, on a system-by-system basis, or perhaps even at the organizational level. In consideration of this flexibility, the extended assessment procedure is applied on an assessment-by-assessment basis typically according to how the organization chose to achieve the associated Special Publication 800-53 assurances for the information system under assessment. Further, the organization selects the appropriate procedural steps from the extended assessment procedure based on the information system impact level. How the organization chooses to apply the procedural steps from the extended procedure, for example, on a per-security-control basis or to a group of security controls (e.g., a set of controls in a particular family of controls), may be different based on the manner in which the organization chooses to achieve the Special Publication 800-53 assurance requirements, but in any case, the method of application should be documented in the security assessment plan. The application of the

extended assessment procedure is intended to supplement the specialized assessment procedures to increase the grounds for confidence that the security controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements of the information system.

Finalize the security assessment plan and obtain approval to execute the plan—

After selecting the assessment procedures (including developing necessary procedures not contained in the NIST Special Publication 800-53A catalog of procedures), tailoring the procedures for information system/platform-specific and organization-specific conditions, optimizing the procedures for efficiency, applying the extended assessment procedure, and addressing the potential for unexpected events impacting the assessment, the assessment plan is finalized and the schedule is established including key milestones for the assessment process. Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials to ensure that the plan is complete, consistent with the security objectives of the organization and the organization's assessment of risk, and cost-effective with regard to the resources allocated for the assessment. After the security assessment plan is approved by the organization, the assessor or assessment team[28] executes the plan in accordance with the agreed-upon milestones and schedule.

3.4 ANALYZING, DOCUMENTING, AND REPORTING ASSESSMENT RESULTS

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the information necessary to make the determination associated with each assessment objective. Each determination statement in a procedural step contained within an assessment procedure executed by an assessor produces one the following findings: (i) satisfied (S); or (ii) other than satisfied (O). A finding of *satisfied* indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result. A finding of *other than satisfied* indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization. A finding of *other than satisfied* may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement. The assessor findings (i.e., the determinations made) should be an objective reporting of what was found concerning the security control assessed. For each finding of *other than satisfied*, assessors should indicate which parts of the security control are affected by the finding (i.e., those aspects of the control that were deemed not satisfied or were not able to be assessed) and describe how the control differs from the planned or expected state. Any potential for compromises to confidentiality, integrity, and availability due to an *other than satisfied* finding should also be noted by the assessor.

The assessment information produced by the assessor (i.e., objective findings of *satisfied* or *other than satisfied*, identification of the parts of the security control that did not produce a satisfactory result, and a description of any resulting potential for compromises to the information system) is provided to the information system owner. Since results of the security assessment ultimately influence the content of the system security plan and the plan of action and milestones, the

[28] Determining the size and organizational makeup of the security assessment team (i.e., skill sets, technical expertise, and assessment experience of the individuals composing the team) is part of the risk management decisions made by the organization requesting and initiating the assessment of the information system.

information system owner reviews the findings of the assessor and coordinates with other organizational officials (e.g., chief information officer, senior agency information security officer, mission/information owners), to determine the appropriate steps required to correct weaknesses and deficiencies identified during the assessment. By using the tags of *satisfied* and *other than satisfied*, the reporting format for the assessment findings provides visibility for organizational officials into specific weaknesses and deficiencies in the information system and facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities.

The information system owner also collaborates with designated organizational officials having an interest in the security assessment to determine the levels of concern regarding the specific weaknesses and deficiencies identified during the assessment. The levels of concern provided by this organizational review of the assessor's findings help establish priorities for remediation activities in the plan of action and milestones. For example, in one instance, the information system owner consults with designated organizational officials and they decide that certain assessment findings marked as *other than satisfied* are of an inconsequential nature and present no significant risk to the organization. Alternatively, the information system owner and organizational officials may decide that certain findings marked as *other than satisfied* are significant, requiring immediate remediation actions. In all cases, the organization reviews each assessor finding of *other than satisfied* and applies its judgment with regard to the severity or seriousness of the finding, that is, the potential adverse affects on organizational operations, organizational assets, individuals, other organizations, or the nation, and whether the finding is significant enough to be worthy of further investigation or remedial action.

The assessor findings are a primary information source for the plan of action and milestones, a document providing a detailed roadmap for correcting the noted weaknesses or deficiencies in the security controls. The assessor does not prepare the plan of action and milestones, but does provide recommendations for its content. The information system owner has an opportunity to address some or all of the weaknesses or deficiencies in the security controls identified during the assessment before those weaknesses or deficiencies become part of the plan of actions and milestones. However, senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in some priority order—first providing resources to the information systems that are supporting the most critical and sensitive missions for the organization. Ultimately, the assessment findings and any subsequent mitigation actions initiated by the information system owner in collaboration with designated organizational officials trigger updates to the risk assessment and the information system security plan. Therefore, the key documents used by the authorizing official to determine the security status of the information system (i.e., system security plan with updated risk assessment, security assessment report, and plan of actions and milestones) are updated to reflect the results of the security assessment.

Security assessment results should be documented at the level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational policy, NIST guidelines, and OMB policy. The reporting format should be consistent with the type of security control assessment conducted including self-assessments by information system owners, independent verification and validation, independent assessments by certification agents or certification teams supporting the security accreditation process, or independent audits of security controls by auditors or inspectors general. A sample reporting format for security assessments is provided in Appendix I. The sample reporting format is illustrative and not intended to limit organizational flexibility in determining the most appropriate presentation for the purposes of a given security assessment.

With respect to supporting the security certification and accreditation process, authorizing officials use the results from the security assessment as one of the critical inputs in helping to decide whether the information system should be authorized for operation or continued in an authorized status. The authorizing official relies on information provided by the information system owner (i.e., the revised risk assessment captured in the updated system security plan and the plan of actions and milestones) along with the objective assessment findings from the assessor (in the security assessment report) in arriving at a decision on the current risk posture and the acceptability of such risk. This is one of the most important decisions for a senior-level official within an organization, given the degree to which organizations now depend on information systems to carry out organizational missions and business functions. To successfully accomplish critical organizational missions and business functions, the information systems supporting those missions and business functions must be dependable in the face of sophisticated and well-resourced, worldwide threats. Having a thorough understanding of the risks to organizational operations and assets, to individuals, to other organizations, and to the nation based on the operation and use of the information system must be a priority for all authorizing officials and senior leaders within the organization. Using information systems wisely to support enterprise-wide missions and business functions in today's environment of sophisticated and well-resourced threat sources, is an imperative for all organizations.

3.5 CONTINUOUS MONITORING OF SECURITY CONTROLS

Conducting a thorough point-in-time assessment of the security controls in an organizational information system is a necessary but not sufficient condition to demonstrate security due diligence. Effective information security programs should also include an aggressive continuous monitoring program to check the status of the security controls in the information system on an ongoing basis. The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. Continuous monitoring, the fourth phase in the security certification and accreditation process, is a proven technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to appropriate organizational officials in order to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective tool for producing ongoing updates to information system security plans, security assessment reports, and POAMs. An effective continuous monitoring program requires:

- Configuration management and control processes for the information system;
- Security impact analyses of changes to the information system;
- Assessment of selected security controls in the information system; and
- Security status reporting to appropriate agency officials.

Organizations should use the current risk assessment, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process. Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., greatest potential for change) after implementation and the controls that have been identified in the organization's POAM for the

information system. Security control volatility is a measure of how frequently a control is likely to change over time after implementation. For example, security policies and implementing procedures in a particular organization may not be likely to change from one year to the next and thus would likely be security controls with lower volatility. Access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of an information system would, therefore, likely be security controls with higher volatility. Organizations will likely apply greater resources to security controls deemed to be of higher volatility as there is typically a higher return on investment for assessing security controls of this type. Security controls identified in the POAM should also be a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree (or nonexistent, in the worst case). In summary, organizations must make informed judgments regarding the application of limited assessment resources when conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorization in accordance with FIPS 199, and testing requirements articulated in federal legislation, policy, directives, and regulations.

As the security certification and accreditation process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the system development life cycle, the ability to update the security assessment report frequently based on the assessment results obtained from the continuous monitoring process becomes a critical aspect of an organization's information security program. It is important to emphasize the relationship, described in NIST Special Publication 800-37, among the three key documents in the accreditation package (i.e., the system security plan including the organizational assessment of risk, the security assessment report, and the plan of action and milestones). It is these documents that provide the best indication of the overall security status of the information system and the ability of the system to protect, to the degree necessary, the organization's operations and assets, individuals, other organizations, and the nation. Updates to these key documents should be provided on an ongoing basis in accordance with the continuous monitoring program established by the organization.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES[29]

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

6. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106 *Designation of Public Trust Positions and Investigative Requirements*, (5 C.F.R. 731.106).
7. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).
8. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
9. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
10. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
11. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
12. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
13. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
14. Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.
15. Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.
16. Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006.

[29] The status and most current versions of NIST publications including FIPS and Special Publications in the 800-series (draft and final) can be found at http://csrc.nist.gov/publications.

STANDARDS

17. International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005.

18. International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005.

19. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

20. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, August 2002.

21. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, January 2000.

22. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

23. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

24. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

25. National Institute of Standards and Technology Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

26. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

27. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

28. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006.

29. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

30. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

GUIDELINES

31. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

32. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.

33. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

34. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC)*, Version 1, September 1997.

35. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

36. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.

37. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

38. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.

39. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, April 2000.

40. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

41. National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001.

42. National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

43. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.

44. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

45. National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

46. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

47. National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

48. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

49. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
50. National Institute of Standards and Technology Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001.
51. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
52. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.
53. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
54. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.
55. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.
56. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
57. National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.
58. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.
59. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.
60. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication* (Draft), April 2006.
61. National Institute of Standards and Technology Special Publication 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005.
62. National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.
63. National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.
64. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.
65. National Institute of Standards and Technology Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002.
66. National Institute of Standards and Technology Special Publication 800-45, *Guidelines on Electronic Mail Security* (Version 2), February 2007.
67. National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

68. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

69. National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

70. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

71. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

72. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

73. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

74. National Institute of Standards and Technology Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

75. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security* (Draft), September 2006.

76. National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

77. National Institute of Standards and Technology Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* (Revised), March 2007.

78. National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management*, Part I: General (Revised), March 2007.

79. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

80. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

81. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

82. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.

83. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, April 2006.

84. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

85. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

86. National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

87. National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

88. National Institute of Standards and Technology Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.

89. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

90. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

91. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

92. National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, March 2006.

93. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

94. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

95. National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.

96. National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

97. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.

98. National Institute of Standards and Technology Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* (Draft), September 2006.

99. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

100. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

101. National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, April 2006.

102. National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006.

103. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

104. National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, March 2007.

105. National Institute of Standards and Technology Special Publication 800-88, *Guidelines For Media Sanitization*, September 2006.

106. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.

107. National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* (Revised), March 2007.

108. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

109. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

110. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services* (Draft), September 2006.

111. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, September 2006.

112. National Institute of Standards and Technology Special Publication 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.

113. National Institute of Standards and Technology Special Publication 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, April 2007.

114. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

115. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics* (Draft), August 2006.

MISCELLANEOUS PUBLICATIONS

116. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.

117. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used within Special Publication 800-53A. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation [FIPS 200, NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Assessment Procedure	One or more procedural steps that are created to achieve a set of assessment objectives by applying assessment methods to assessment objects.
Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.

Authorize Processing	See Accreditation.
Authorizing Official [FIPS 200, NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.
Certification [FIPS 200, NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Controlled Area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type).

Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Extended Assessment Procedure	A type of assessment procedure that is applied to an individual security control or a group of controls (e.g., the set of security controls in a particular security control family or the set of controls in an information system security plan) and is used in conjunction with specialized assessment procedures in providing the necessary information for determining control effectiveness.
External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Guard (System) [CNSS Inst. 4009, Adapted]	A mechanism limiting the exchange of information between information systems or subsystems.

High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control [NIST SP 800-53]	Security control for an information system where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Label	See Security Label.
Line of Business	The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.
Local Access	Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Major Information System [OMB Circular A-130]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Malicious Code [CNSS Inst. 4009] [NIST SP 800-61]	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See Malicious Code.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Media Access Control Address	A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.
Media Sanitization [NIST SP 800-88]	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Function	A function executed on an information system involving the control, monitoring, or administration of the system.
Privileged User [CNSS Inst. 4009]	Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer).
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).
Risk [FIPS 200, Adapted]	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30, Adapted]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls.

Risk Management [FIPS 200]	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline [FIPS 200]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Functions	The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Incident	See Incident.

Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Perimeter	See Accreditation Boundary.
Security Plan	See System Security Plan.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Specialized Assessment Procedure	A type of assessment procedure that is applied to an individual security control and used in conjunction with an extended assessment procedure in obtaining the information necessary for determining control effectiveness.
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System-specific Security Control [NIST SP 800-37]	Security control for an information system that has not been designated as a common security control.

Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.
Tailored Security Control Baseline	Set of security controls resulting from the application of the tailoring guidance in NIST Special Publication 800-53 to the security control baseline.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can be activated only by the user or the security functions of the information system and cannot be imitated by untrusted software.
User [CNSS Inst. 4009]	Individual or (system) process authorized to access an information system.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
COTS	Commercial Off-The-Shelf
DCID	Director of Central Intelligence Directive
DNS	Domain Name System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
ISAP	Information Security Automation Program
IPsec	Internet Protocol Security
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information System Security Instruction
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SP	Special Publication
ST&E	Security Test and Evaluation
TCP/IP	Transmission Control Protocol/Internet Protocol
TSP	Telecommunications Service Priority
U.S.C.	United States Code
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
VOIP	Voice Over Internet Protocol

APPENDIX D

ASSESSMENT METHOD DESCRIPTIONS

ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

This appendix provides complete definitions of the three assessment methods that can be used by assessors during security assessments: (i) *examine*; (ii) *interview*; and (iii) *test*. The definitions include a set of attributes and attribute values for each of the assessment methods. The attribute values for the assessment methods (which describe the rigor and level of detail associated with the assessment) are hierarchical in nature.[30] For the depth attribute, the *focused* attribute value includes and builds upon the assessment rigor and level of detail defined for the *generalized* attribute value; the *detailed* attribute value includes and builds upon the assessment rigor and level of detail defined for the *focused* attribute value. For the coverage attribute, the *specific* attribute value includes and builds upon the number and type of assessment objects defined for the *representative* attribute value; the *comprehensive* attribute value includes and builds upon the number and type of assessment objects defined for the *specific* attribute value. The use of **bolded text** in the assessment method descriptions indicates the content that was added to the attribute value descriptions and appears for the first time.

[30] The hierarchical nature of the attribute values for the assessment methods is used to increase the breadth and depth of the assessment evidence collected during the assessment to support the increased assurances that are needed for higher impact level information systems (see Table E-2, Appendix E).

ASSESSMENT METHOD: Examine

ASSESSMENT OBJECTS: Specifications (e.g., policies, plans, procedures, system requirements, designs)
Mechanisms (e.g., functionality implemented in hardware, software, firmware)
Activities (e.g., system operations, administration, management; exercises)

DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations, reviewing the results of contingency plan exercises; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the information system hardware/software; or checking, studying, or observing physical security measures related to the operation of an information system.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) *generalized*; (ii) *focused*; and (iii) *detailed*.
  - Generalized examination: Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions) to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors.
  - Focused examination: Examination that consists of high-level reviews, checks, observations, or inspections **and more in depth analyses** of the assessment object **deemed particularly important to achieving the assessment objective**. This type of examination is conducted using a **substantial** body of evidence or documentation (e.g., functional-level descriptions and **where appropriate and available, high-level design information**) to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Detailed examination: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth, **detailed, and thorough** analyses of the assessment object deemed particularly important to achieving the assessment objective. This type of examination is conducted using an **extensive** body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information, **low-level design information, and implementation information**) to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.
- The *coverage* attribute addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined, the number of objects to be examined (by type), and specific objects to be examined.[31] There are three possible values for the coverage attribute: (i) *representative*, (ii) *specific*, and (iii) *comprehensive*.
  - Representative examination: Examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

[31] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be examined for the particular attribute value described.

- Specific examination: Examination that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
- Comprehensive examination: Examination that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

ASSESSMENT METHOD: Interview

ASSESSMENT OBJECTS: Individuals or groups of individuals.

DEFINITION: The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control existence, functionality, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example, interviewing agency heads, chief information officers, senior agency information security officers, authorizing officials, information owners, information system and mission owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) *generalized*; (ii) *focused*; and (iii) *detailed*.
  - Generalized interview: Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors.
  - Focused interview: Interview that consists of broad-based, high-level discussions **and more in depth discussions in specific areas** with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions **and more in depth questions in specific areas where responses indicate a need for more in depth investigation** to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Detailed interview: Interview that consists of broad-based, high-level discussions and more in depth, **probing** discussions in specific areas **(including other assessment results)** with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth, **probing** questions in specific areas where responses indicate a need for more in depth investigation **or where called for by assessment procedures** to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.
- The *coverage* attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed.[32] There are three possible values for the coverage attribute: (i) *representative*, (ii) *specific*, and (iii) *comprehensive*.
  - Representative interview: Interview that uses a representative sample of individuals in key organizational roles to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.
  - Specific interview: Interview that uses a representative sample of individuals in key organizational roles **and other specific individuals deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.

[32] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific individuals to be interviewed for the particular attribute value described.

- Comprehensive interview: Interview that uses a **sufficiently large** sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

ASSESSMENT METHOD: Test

ASSESSMENT OBJECTS: Mechanisms (e.g., hardware, software, firmware)
Activities (e.g., system operations, administration, management; exercises)

DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, and potential for improvement over time.[33]

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: testing access control, identification and authentication, and audit mechanisms; testing security configuration settings; testing physical access control devices; conducting penetration testing of key information system components; testing information system backup operations; testing incident response capability; and exercising contingency planning capability.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the types of testing to be conducted. There are three possible values for the depth attribute: (i) *generalized* testing; (ii) *focused* testing; and (iii) *detailed* testing.
  - Generalized testing: Test methodology (also known as *black box* testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors.
  - Focused testing: Test methodology (also known as ***gray box*** testing) that assumes **some** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification **and limited system architectural information (e.g., high-level design)** to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Detailed testing: Test methodology (also known as *white box* testing) that assumes **explicit and substantial** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, **extensive** system architectural information (e.g., high-level design, **low-level design) and implementation representation (e.g., source code, schematics)** to provide a level of understanding of the security control functionality and implementation necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.
- The *coverage* attribute addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested, the number of objects to be tested (by type), and specific objects to be tested.[34] There are three possible values for the coverage attribute: (i) *representative*; (ii) *specific*; and (iii) *comprehensive*.
  - Representative testing: Testing that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

[33] Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security control that are not commonly associated with predefined specifications, with an example of such testing being penetration testing. Guidelines for conducting penetration testing are provided in Appendix G.

[34] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be tested for the particular attribute value described. For mechanism-related testing, the coverage attribute also addresses the extent of the testing conducted (e.g., for software, the number of test cases and modules tested; for hardware, the range of inputs, number of components tested, and range of environmental factors over which the testing is conducted).

- Specific testing: Testing that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
- Comprehensive testing: Testing that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

APPENDIX E

ASSESSMENT EXPECTATIONS

CHARACTERIZING THE EXPECTATIONS OF SECURITY ASSESSMENTS BY IMPACT LEVEL

The following section establishes the expectations for security control assessments based on the assurance requirements defined in NIST Special Publication 800-53. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. The use of **bolded text** in the assurance requirements and assessment objectives in this section indicates additions to the requirements and objectives that appear for the first time at a particular information system impact level.

LOW-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement.

Supplemental Guidance: For security controls in low-impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Assessment Expectations: Generalized interviews, examinations, and tests are conducted using a representative set of assessment objects to demonstrate that the security control is implemented and free of obvious errors.

Assessment Objectives:

For *specifications*:

- Determine if the specification exists.
- Determine if the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.

For *mechanisms*:

- Determine if the mechanism is implemented and operational.
- Determine if the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.

For *activities*:

- Determine if the activity is being performed.
- Determine if the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious execution errors.

MODERATE-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in moderate-impact information systems, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

Assessment Expectations: **Focused** interviews, examinations, and tests are conducted using a **specific** set of assessment objects to demonstrate that the security control is implemented and free of obvious errors, **and that there are increased grounds for confidence that the security control is implemented correctly and operating as intended**.

Assessment Objectives:

For *specifications:*

- Determine if the specification exists.
- Determine if the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.
- **Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the specification is complete, internally consistent, correct, and meets its required function or purpose.**
- **Determine if the organization identifies and documents anomalies or problems with the application or use of the specification.**

For *mechanisms*:

- Determine if the mechanism is implemented and operational.
- Determine if the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.
- **Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the mechanism is implemented correctly, operating as intended, and meets its required function or purpose.**
- **Determine if the organization identifies and documents anomalies or problems with the implementation or operation of the mechanism.**

For *activities*:

- Determine if the activity is being performed.
- Determine if the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious execution errors.
- **Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the activity is being performed correctly and meets its required function or purpose.**
- **Determine if the organization identifies and documents anomalies or problems with the conduct or execution of the activity.**

HIGH-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis and testing of the control (**including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in high-impact information systems, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Assessment Expectations: **Detailed** interviews, examinations, and tests are conducted using a **comprehensive** set of assessment objects to demonstrate that the security control is implemented and free of obvious errors and that there are further increased grounds for confidence that the security control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

Assessment Objectives:

For *specifications:*

- Determine if the specification exists.
- Determine if the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.
- Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the specification is complete, internally consistent, correct, and meets its required function or purpose.
- Determine if the organization identifies and documents anomalies or problems with the application or use of the specification.
- **Determine if the organization applies the specification consistently across the information system.**
- **Determine if the organization supports improvement in the effectiveness of the specification by taking specific actions to correct identified deficiencies.**

For *mechanisms*:

- Determine if the mechanism is implemented and operational.
- Determine if the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.
- Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the mechanism is implemented correctly, operating as intended, and meets its required function or purpose.
- Determine if the organization identifies and documents anomalies or problems with the implementation or operation of the mechanism.
- **Determine if the organization implements the mechanism consistently across the information system.**
- **Determine if the organization supports improvement in the effectiveness of the mechanism by taking specific actions to correct identified deficiencies.**

For *activities*:

- Determine if the activity is being performed.
- Determine if the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious execution errors.
- Determine if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the activity is being performed correctly and meets its required function or purpose.
- Determine if the organization identifies and documents anomalies or problems with the conduct or execution of the activity.
- **Determine if the organization performs the activity consistently across the information system.**
- **Determine if the organization supports improvement in the effectiveness of the activity by taking specific actions to correct identified deficiencies.**

ADDITIONAL REQUIREMENTS TO SUPPLEMENT MODERATE- AND HIGH-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. *This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.*

Table E-1 provides a summary of the assessment expectations for low-impact, moderate-impact, and high-impact information systems.

TABLE E-1: ASSESSMENT EXPECTATIONS BY INFORMATION SYSTEM IMPACT LEVEL

ASSESSMENT EXPECTATIONS	INFORMATION SYSTEM IMPACT LEVEL		
	LOW	MODERATE	HIGH
Security controls are in place with no obvious errors.	√	√	√
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	---	√	√
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	---	---	√
Grounds for a high degree of confidence that the security controls are complete, consistent, and correct. ***Beyond minimum recommendations of Special Publication 800-53A***	*For environments with specific and credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets.*		

Table E-2 provides a summary of the assessment method attributes and attribute values described in Appendix D by information system impact level. The associated value assigned to a particular attribute provides a direct link to the assurance requirements in NIST Special Publication 800-53.

TABLE E-2: ASSESSMENT METHOD ATTRIBUTES AND ATTRIBUTE VALUES BY IMPACT LEVEL

ASSESSMENT METHODS Examine, Interview, Test	**INFORMATION SYSTEM IMPACT LEVEL**		
ATTRIBUTE	**LOW**	**MODERATE**	**HIGH**
Depth	*Generalized*	*Focused*	*Detailed*
Coverage[35]	*Representative*	*Specific*	*Comprehensive*

[35] The types and number of assessment objects included in the assessment should be a function of the FIPS 199 impact level of the information system. Organizations should consider increasing the types and number of objects assessed as the impact level of the information system increases. The increased depth and coverage of the assessment contributes to greater assurance in the overall effectiveness of the security controls under assessment.

APPENDIX F

ASSESSMENT PROCEDURE CATALOG

METHODS, OBJECTS, AND OBJECTIVES FOR ASSESSING SECURITY CONTROLS

This appendix provides a catalog of *specialized assessment procedures* to assess the security controls and control enhancements in NIST Special Publication 800-53.[36] The catalog also contains one *extended assessment procedure* that is employed by assessors to obtain additional evidence to support the grounds for confidence that the security controls are effective in their application. The specialized assessment procedures are organized by families similar to the security control catalog in Special Publication 800-53. The extended assessment procedure, which follows the specialized assessment procedures in the catalog, can be applied by the organization in a variety of ways depending on how the information system security controls are developed and implemented, and how the organization manages its security assessment processes. Section 3.3 of this document provides guidance on the application of the extended assessment procedure.

Each assessment procedure consists of one or more procedural steps, which are used in assessing particular aspects of a security control or control enhancement (or in the case of the extended assessment procedure, aspects of the security control, control enhancement, family of controls, or security controls employed across the organization). Each procedural step in an assessment procedure contains a unique identifier. For example, CP-3.2 indicates that this is the second step used to assess security control CP-3. CP-4 (2).1 indicates that this is the first step used to assess the second enhancement for security control CP-4. The extended assessment procedural steps are numbered sequentially (i.e., EAP.1, EAP.2, EAP.3, EAP.4, EAP.5) and are employed based upon the impact level of the information system.

Assessors select the appropriate assessment procedures from the catalog for the security controls and control enhancements described in the information system security plan that are to be assessed in a particular assessment. It should be recognized, therefore, that there will likely be assessment procedures in the catalog that assessors will not use because: (i) the associated security control or control enhancement is not described in the security plan for the information system; or (ii) the security control or control enhancement is not being assessed at a given time (e.g., during an assessment related to continuous monitoring activities).

Recognizing that organizations can specify, organize, document, and configure their information systems in a variety of ways, the assessment objects identified in Appendix F that are used in conjunction with the interview, examine, and test methods should be considered suggested objects where information/evidence may be found. As such, assessors are expected to use their judgment in applying the designated assessment methods to the associated set of assessment objects. Each assessment method listed in a procedural step should be applied to a sufficient number of identified (or additional) assessment objects as appropriate to produce the information necessary to make the determination in the determination statement and to satisfy the assessment objective. ***It may not always be necessary to apply each assessment method to every assessment object in the list***.

[36] For ease of use and quick reference, a description of the specific security control or control enhancement from NIST Special Publication 800-53 under assessment is provided in the shaded grey area at the beginning of the associated assessment procedure.

Implementation Tips

TIP #1: For each assessment step, in both the specialized and extended assessment procedures, each assessment method begins with the text (DEPTH, COVERAGE). The assessor selects and applies to each method, the attribute values for depth and coverage that are appropriate to the impact level of the information system that is being assessed (see Table E-2 in Appendix E).

TIP #2: The determination statements and assessment methods marked with an "L" or and "M" in the catalog of assessment procedures in Appendix F indicates use of the determination statements or assessment methods is optional for low-impact and moderate-impact information systems, respectively. Section 3.3 of this document provides guidance on the application of the "L" or and "M" marked statements or assessment methods.

Section I: Specialized Assessment Procedures

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-1 ACCESS CONTROL POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents access control policy and procedures;* *(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review access control policy and procedures; and* *(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with access control responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
AC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with access control responsibilities. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-2 ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*]. Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
AC-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;* *(ii) the organization defines the frequency of information system account reviews;* *(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and* *(iv) the organization initiates required actions on information system accounts based on the review.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with account management responsibilities. (L)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: **(1) The organization employs automated mechanisms to support the management of information system accounts.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to support information system account management functions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; account management procedures; information system design documentation, information system configuration settings and associated documentation; list of account management functions; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing account management functions. (M)
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: **(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a time period after which the information system terminates temporary and emergency accounts; and* *(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; account management procedures; information system security plan (for organization-defined time period for automatic account termination by account type); information system design documentation, information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing account management functions. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: **(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a time period after which the information system disables inactive accounts; and* *(ii) the information system automatically disables inactive accounts after organization-defined time period.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; account management procedures; information system security plan (for organization-defined time period for automatic account disabling); information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing account management functions. (M)
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: **(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing account management functions. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-3 ACCESS ENFORCEMENT Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Related security control: SC-13. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and* *(ii) user privileges on the information system are consistent with the documented user authorizations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access enforcement policy and procedures; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access enforcement policy. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-3 ACCESS ENFORCEMENT Control Enhancement: **(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.** Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers). (M) Indicates that this section of the assessment procedure is optional for moderate-impact and low-impact systems.
AC-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization explicitly defines privileged functions and security-relevant information for the information system;* *(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and* *(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access enforcement policy. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-4 INFORMATION FLOW ENFORCEMENT Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Related security control: SC-7. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information flow enforcement policy and procedures; information system design documentation; information system baseline configuration; information system configuration settings and associated documentation; list of information flow authorizations; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information flow enforcement policy. (M)
AC-4.2	**ASSESSMENT OBJECTIVE:** *Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system interconnection agreements; information flow enforcement policy; information system configuration settings and associated documentation; list of information flow control authorizations; information system audit records; other relevant documents or records.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-4 INFORMATION FLOW ENFORCEMENT Control Enhancement: **(1) The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.** Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.
AC-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information flow enforcement policy and procedures; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information flow enforcement policy.
	AC-4 INFORMATION FLOW ENFORCEMENT Control Enhancement: **(2) The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.**
AC-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information flow enforcement policy and procedures; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information flow enforcement policy.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-4 INFORMATION FLOW ENFORCEMENT Control Enhancement: **(3) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.**
AC-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information flow enforcement policy and procedures; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information flow enforcement policy.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and* *(ii) the information system enforces separation of duties through assigned access authorizations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties. (M) **Test** (DEPTH, COVERAGE): Automated mechanisms implementing separation of duties policy. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-6 LEAST PRIVILEGE Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and* *(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-7 UNSUCCESSFUL LOGIN ATTEMPTS Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded. Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;* *(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;* *(iii) the organization defines the time period for lock out mode or delay period;* *(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts;* *(v) the information system enforces the organization-selected lock out mode or delayed login prompt.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing unsuccessful logon attempts; information system security plan (for organization-defined maximum number of invalid access attempts within organization-defined time period, automatic response when maximum number of invalid access attempts is exceeded, time period for lock out mode or delay period); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for unsuccessful login attempts. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-7 UNSUCCESSFUL LOGIN ATTEMPTS Control Enhancement: **(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.**
AC-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful login attempts is exceeded.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing unsuccessful logon attempts; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for unsuccessful login attempts.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-8 SYSTEM USE NOTIFICATION Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system. Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system displays a system use notification message before granting system access informing potential users:* *- that the user is accessing a U.S. Government information system;* *- that system usage may be monitored, recorded, and subject to audit;* *- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;* *- that use of the system indicates consent to monitoring and recording;* *(ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).* *(iii) the organization approves the information system use notification message before its use; and* *(iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for system use notification. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-9 PREVIOUS LOGON NOTIFICATION Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon. Supplemental Guidance: None.
AC-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, upon successful logon, displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing previous logon notification; information system notification messages; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for previous logon notification.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-10 CONCURRENT SESSION CONTROL Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*]. Supplemental Guidance: None.
AC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of concurrent sessions for information system users; and* *(ii) the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan (for organization-defined limit for concurrent sessions for information system users); other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for concurrent session control.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-11 SESSION LOCK Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of user inactivity that initiates a session lock within the information system;* *(ii) the information system initiates a session lock after the organization-defined time period of inactivity; and* *(iii) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session lock is to be activated); other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for session lock. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-12 SESSION TERMINATION Control: The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity. Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of user inactivity that initiates a remote session termination within the information system; and* *(ii) the information system automatically terminates a remote session after the organization-defined time period of inactivity.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan (for organization-defined time period for user inactivity after which automatic session termination is to be activated); other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for session termination. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-12 SESSION TERMINATION Control Enhancement: **(1) Automatic session termination applies to local and remote sessions.**
AC-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if automatic session termination applies to local and remote sessions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for session termination.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-13.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with supervisory and access control responsibilities. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL Control Enhancement: **(1) The organization employs automated mechanisms to facilitate the review of user activities.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting the access control policy for supervision and review of user activities. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov). Related security control: IA-2. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for permitted actions without identification and authentication. (L) (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control Enhancement: **(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibilities for defining permitted actions without identification and authentication. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-15 AUTOMATED MARKING Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions. Supplemental Guidance: Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.
AC-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies standard naming conventions for information system output; and* *(ii) the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures for addressing automated marking of information system output; information system output; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing automated marking of information system output.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-16 AUTOMATED LABELING Control: The information system appropriately labels information in storage, in process, and in transmission. Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.
AC-16.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system appropriately labels information in storage, in process, and in transmission.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing automated (internal) labeling within the information system.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-17 REMOTE ACCESS Control: The organization authorizes, monitors, and controls all methods of remote access to the information system. Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
AC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization documents, monitors, and controls all methods of remote access to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with remote access authorization, monitoring, and control responsibilities. (L)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-17 REMOTE ACCESS Control Enhancement: **(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-17(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for remote access. (M)
	AC-17 REMOTE ACCESS Control Enhancement: **(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-17(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing cryptographic protections for remote access. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-17 REMOTE ACCESS Control Enhancement: **(3) The organization controls all remote accesses through a limited number of managed access control points.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-17(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines managed access control points for remote access to the information system; and* *(ii) the information system controls all remote accesses through a limited number of managed access control points.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for remote access. (M)
	AC-17 REMOTE ACCESS Control Enhancement: **(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-17(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and* *(ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for remote access. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-18 WIRELESS ACCESS RESTRICTIONS Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system. Supplemental Guidance: NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
AC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;* *(ii) the organization authorizes, monitors, and controls wireless access to the information system; and* *(iii) the wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST Special Publications 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Wireless access usage and restrictions. (L)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-18 WIRELESS ACCESS RESTRICTIONS Control Enhancement: **(1) The organization uses authentication and encryption to protect wireless access to the information system.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses authentication and encryption to protect wireless access to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the access control policy for wireless access to the information system. (M)
	AC-18 WIRELESS ACCESS RESTRICTIONS Control Enhancement: **(2) The organization scans for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if such an access points are discovered.** Enhancement Supplemental Guidance: Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.
AC-18(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of scans for unauthorized wireless access points; and* *(ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access points are discovered.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system configuration settings and associated documentation; wireless scanning reports; other relevant documents or records. **Test** (DEPTH, COVERAGE): Scanning procedure for unauthorized wireless access points.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems. Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;* *(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and* *(iii) the organization authorizes, monitors, and controls device access to organizational information systems.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel who use portable and mobile devices to access the information system. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access control policy for portable and mobile devices. (M)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system. Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
AC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of applications that can be accessed from the external information system;* *(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and* *(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel who use external information systems to access the information system. (L)

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS Control Enhancement: **(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.**
AC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:* - *verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when allowing connections to the external information system; or* - *approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; list of information system accounts; other relevant documents or records.

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AT-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents security awareness and training policy and procedures;* *(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and* *(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security awareness and training responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
AT-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security awareness and training responsibilities. (L) (M)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AT-2 SECURITY AWARENESS Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter. Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AT-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes;* *(ii) the security awareness training is consistent with applicable regulations and NIST Special Publication 800-50;* (L) *(iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;* (L) *(iv) the organization defines the frequency of refresher security awareness training; and* *(v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy; procedures addressing security awareness training implementation; NIST Special Publication 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan (for organization-defined frequency of refresher security awareness training); other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel comprising the general information system user community. (L) (M)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AT-3 SECURITY TRAINING Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter. Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AT-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;* *(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;* *(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;* (L) *(iv) the security training is consistent with applicable regulations and NIST Special Publication 800-50;* (L) *(v) the organization defines the frequency of refresher security training; and* *(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy; procedures addressing security training implementation; NIST Special Publication 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with significant information system security responsibilities. (L) (M)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AT-4 SECURITY TRAINING RECORDS Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. Supplemental Guidance: None.
AT-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization monitors and documents basic security awareness training and specific information system security training.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents. Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
AT-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and share security-related information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents audit and accountability policy and procedures;* *(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and* *(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with audit and accountability responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
AU-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with audit and accountability responsibilities. (L) (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-2 AUDITABLE EVENTS Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*]. Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system auditable events;* *(ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and* *(iii) the information system generates audit records for the organization-defined auditable events.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system auditing of organization-defined auditable events. (L) (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-2 AUDITABLE EVENTS Control Enhancement: **(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.**
AU-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the components of the information system that generate audit records; and* *(ii) the information system compiles audit records from the organization-defined (multiple) components within the information system into a systemwide (logical or physical), time-correlated audit trail.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing auditable events; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing a system-wide auditing capability.
	AU-2 AUDITABLE EVENTS Control Enhancement: **(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.**
AU-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing auditable events; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing Information system auditing for the specified components of the information system.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-2 AUDITABLE EVENTS Control Enhancement: **(3) The organization periodically reviews and updates the list of organization-defined auditable events.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization periodically reviews and updates the list of organization-defined auditable events.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing auditable events; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with auditing and accountability responsibilities. (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-3 CONTENT OF AUDIT RECORDS Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-3.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system auditing of auditable events with organization-defined audit record content. (L) (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-3 CONTENT OF AUDIT RECORDS Control Enhancement: **(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing the content of audit records; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject. (M)
	AU-3 CONTENT OF AUDIT RECORDS Control Enhancement: **(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.**
AU-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to centrally manage the content of audit records generated from multiple components throughout the system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing the content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system auditing with central management capability.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-4 AUDIT STORAGE CAPACITY Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.
AU-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines audit record storage capacity for the information system components that generate audit records; and* *(ii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-5 RESPONSE TO AUDIT PROCESSING FAILURES Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*]. Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines actions to be taken in the event of an audit processing failure;* *(ii) the organization defines personnel to be notified in case of an audit processing failure; and* *(iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system response to audit processing failures. (L) (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-5 RESPONSE TO AUDIT PROCESSING FAILURES Control Enhancement: **(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].**
AU-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines percentage of maximum audit record storage capacity;* *(ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for organization-defined percentage of maximum audit record storage capacity); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing audit storage limit warnings.
	AU-5 RESPONSE TO AUDIT PROCESSING FAILURES Control Enhancement: **(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].**
AU-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines audit failure events requiring real-time alerts; and* *(ii) the information system provides a real-time alert when organization-defined audit failure events occur.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for organization-defined audit failure events requiring real-time alerts); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing real time audit alerts.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;* *(ii) the organization investigates suspicious activity or suspected violations;* *(iii) the organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials; and* *(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system audit monitoring, analysis, and reporting capability. (M)
AU-6.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities. (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING Control Enhancement: **(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.**
AU-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities.
	AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING Control Enhancement: **(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].**
AU-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines inappropriate or unusual activities with security implications; and* *(ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan (for list of organization-defined inappropriate or unusual activities with security implications); information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing security alerts.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-7 AUDIT REDUCTION AND REPORT GENERATION Control: The information system provides an audit reduction and report generation capability. Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides an audit reduction and report generation capability.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities. (M) **Test** (DEPTH, COVERAGE): Audit reduction and report generation capability.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-7 AUDIT REDUCTION AND REPORT GENERATION Control Enhancement: **(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Audit reduction and report generation capability. (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-8 TIME STAMPS Control: The information system provides time stamps for use in audit record generation. Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
AU-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides time stamps for use in audit record generation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing time stamp generation. (L)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-8 TIME STAMPS Control Enhancement: **(1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of internal clock synchronization for the information system; and* *(ii) the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing time stamp generation; information system security plan (for organization-defined frequency for internal clock synchronization for the information system); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing internal information system clock synchronization. (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-9 PROTECTION OF AUDIT INFORMATION Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit information protection; access control policy and procedures; media protection policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing audit information protection. (L) (M)

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-9 PROTECTION OF AUDIT INFORMATION Control Enhancement: **(1) The information system produces audit records on hardware-enforced, write-once media.**
AU-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system produces audit information on hardware-enforced, write-once media.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit information protection; access control policy and procedures; media protection policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Media storage devices.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-10 NON-REPUDIATION Control: The information system provides the capability to determine whether a given individual took a particular action. Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).
AU-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing non-repudiation capability.

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	AU-11 AUDIT RECORD RETENTION Control: The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit record retention. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
AU-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the retention period for audit records generated by the information system; and* *(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system audit record retention responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls. Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;* *(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review policy and procedures; and* *(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security assessment and certification and accreditation policies and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security assessment and certification and accreditation responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
CA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security assessment and certification and accreditation policies and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security assessment and certification and accreditation responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-2 SECURITY ASSESSMENTS Control: The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system. OMB does not require an annual assessment of *all* security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST Special Publication 800-53A provides guidance on security control assessments to include reuse of existing assessment results. Related security controls: CA-4, CA-6, CA-7, SA-11.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
CA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system is in the inventory of major information systems; and* *(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security assessment policy; procedures addressing security assessments; information system security plan (for organization-defined frequency of security control assessments); security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-3 INFORMATION SYSTEM CONNECTIONS Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis. Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);* *(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;* *(iii) the organization monitors/controls the system interconnections on an ongoing basis; and* *(iv) information system connection agreements are consistent with NIST Special Publication 800-47.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Access control policy; procedures addressing information system connections; NIST Special Publication 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-4 SECURITY CERTIFICATION Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. Related security controls: CA-2, CA-6, SA-11. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and* *(ii) the organization employs a security certification process in accordance with OMB policy and NIST Special Publications 800-37 and 800-53A.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security certification responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-4 SECURITY CERTIFICATION Control Enhancement: **(1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.** Enhancement Supplemental Guidance: An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.
CA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-5 PLAN OF ACTION AND MILESTONES Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. Supplemental Guidance: The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system; and* *(ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy and procedures; information system security plan (for organization-defined frequency of plan of action and milestones updates); security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with plan of action and milestones development and implementation responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-6 SECURITY ACCREDITATION Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation. Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. Related security controls: CA-2, CA-4, CA-7. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three years;* *(ii) a senior organizational official signs and approves the security accreditation;* *(iii) the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37; and* *(iv) the organization updates the authorization when there is a significant change to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing security accreditation; NIST Special Publication 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security accreditation responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-7 CONTINUOUS MONITORING Control: The organization monitors the security controls in the information system on an ongoing basis. Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2). This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
CA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization monitors the security controls in the information system on an ongoing basis; and* *(ii) the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A;* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST Special Publications 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with continuous monitoring responsibilities. (L) (M)
CA-7.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts security impact analyses on changes to the information system;* *(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and* *(iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with continuous monitoring responsibilities. (L) (M)

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CA-7 CONTINUOUS MONITORING Control Enhancement: **(1) The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.** Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.
CA-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with continuous monitoring responsibilities.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CM-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents configuration management policy and procedures;* *(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review configuration management policy and procedures; and* *(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with configuration management and control responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
CM-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with configuration management and control responsibilities. (L) (M)

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system. Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
CM-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops, documents, and maintains a baseline configuration of the information system;* *(ii) the baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architecture;* (L) *(iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built;* (L) *and* *(iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-2 BASELINE CONFIGURATION Control Enhancement: **(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.**
CM-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and* *(ii) the organization updates the baseline configuration of the information system as an integral part of information system component installations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records.
	CM-2 BASELINE CONFIGURATION Control Enhancement: **(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.**
CM-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing baseline configuration maintenance.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-3 CONFIGURATION CHANGE CONTROL Control: The organization authorizes, documents, and controls changes to the information system. Supplemental Guidance: The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system. Related security controls: CM-4, CM-6, SI-2. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CM-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization authorizes, documents, and controls changes to the information system;* *(ii) the organization manages configuration changes to the information system using an organizationally approved process;* *(iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and* *(iv) the organization audits activities associated with configuration changes to the information system.* (M) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-3 CONFIGURATION CHANGE CONTROL Control Enhancement: **(1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.**
CM-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to document proposed changes to the information system;* *(ii) the organization employs automated mechanisms to notify appropriate approval authorities;* *(iii) the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner;* *(iv) the organization employs automated mechanisms to inhibit change until necessary approvals are received; and* *(v) the organization employs automated mechanisms to document completed changes to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing configuration change control.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-4 MONITORING CONFIGURATION CHANGES Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes. Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security control: CA-7.
CM-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the types of information system changes to be monitored;* *(ii) the organization monitors changes to the information system; and* *(iii) the organization conducts security impact analyses to assess the effects of the information system changes.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-5 ACCESS RESTRICTIONS FOR CHANGE Control: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes. Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CM-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes;* *(ii) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and* *(iii) the organization generates, retains, and reviews records reflecting all such changes to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Change control process and associated restrictions for changes to the information system. (M)

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-5 ACCESS RESTRICTIONS FOR CHANGE Control Enhancement: **(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.**
CM-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access restrictions for changes to the information system.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-6 CONFIGURATION SETTINGS Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system. Supplemental Guidance: Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related security controls: CM-2, CM-3, SI-4. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
CM-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;* *(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;* *(iii) the organization documents the configuration settings; and* *(iv) the organization enforces the configuration settings in all components of the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST Special Publication 800-70; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system configuration settings. (L)

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-6 CONFIGURATION SETTINGS Control Enhancement: **(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.**
CM-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs automated mechanisms to centrally manage, apply, and verify configuration settings.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the centralized management, application, and verification of configuration settings.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-7 LEAST FUNCTIONALITY Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*]. Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).
CM-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system;* *(ii) the organization configures the information system to provide only essential capabilities; and* *(iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system configuration settings.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-7 LEAST FUNCTIONALITY Control Enhancement: **(1) The organization reviews the information system [*Assignment: organization-defined frequency*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.**
CM-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of the information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services; and* *(ii) the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services in accordance with the organizational defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for organization-defined frequency for information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services); information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.
CM-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops, documents, and maintains a current inventory of the components of the information system; and* *(ii) the inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control Enhancement: **(1) The organization updates the inventory of information system components as an integral part of component installations.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CM-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization updates the inventory of information system components as an integral part of component installations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system installation and inventory responsibilities. (M)
	CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control Enhancement: **(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.**
CM-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Configuration management policy; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system component inventory management.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents contingency planning policy and procedures;* *(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and* *(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
CP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities. (L) (M)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-2 CONTINGENCY PLAN Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel. Supplemental Guidance: None. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents a contingency plan for the information system;* *(ii) the contingency plan is consistent with NIST Special Publication 800-34;* (L) *(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;* *(iv) the contingency plan is reviewed and approved by designated organizational officials; and* *(v) the organization disseminates the contingency plan to key contingency personnel.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; procedures addressing contingency operations for the information system; NIST Special Publication 800-34; contingency plan; other relevant documents or records.
CP-2.2	**ASSESSMENT OBJECTIVE:** *Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities. (L)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-2 CONTINGENCY PLAN Control Enhancement: **(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.** Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.
CP-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.
	CP-2 CONTINGENCY PLAN Control Enhancement: **(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.**
CP-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-3 CONTINGENCY TRAINING Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*]. Supplemental Guidance: None.
CP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides contingency training to personnel with significant contingency roles and responsibilities;* *(ii) the organization records the type of contingency training received and the date completed;* *(iii) the organization defines frequency of refresher contingency training; and* *(iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan (for organization-defined frequency for refresher contingency training); other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning, plan implementation, and training responsibilities.
CP-3.2	**ASSESSMENT OBJECTIVE:** *Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-3 CONTINGENCY TRAINING Control Enhancement: **(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.**
CP-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization incorporates simulated events into contingency training; and* *(ii) the training is effective in getting organizational personnel to respond as expected to simulated crisis situations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning, plan implementation, and training responsibilities.
	CP-3 CONTINGENCY TRAINING Control Enhancement: **(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.**
CP-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms for contingency training; and* *(ii) the automated mechanisms improve the effectiveness of the contingency training.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency training; automated mechanisms supporting contingency training; contingency training curriculum; contingency training material; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning, plan implementation, and training responsibilities.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES Control: The organization: (i) tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions. Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.
CP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of contingency plan tests and/or exercises;* *(ii) the organization defines the set of contingency plan tests and/or exercises;* *(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;* *(iv) the organization documents the results of contingency plan testing/exercises; and* *(v) the organization reviews the contingency plan test/exercise results and takes corrective actions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records.
CP-4.2	**ASSESSMENT OBJECTIVE:** *Determine if the contingency plan tests/exercises address key aspects of the plan.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES Control Enhancement: **(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.** Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.
CP-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning, plan implementation, and testing responsibilities.
	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES Control Enhancement: **(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.**
CP-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES Control Enhancement: **(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.**
CP-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms for contingency plan testing/exercises; and* *(ii) the automated mechanisms improve the effectiveness of the contingency plan testing/exercises.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-5 CONTINGENCY PLAN UPDATE Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan). (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
CP-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of contingency plan reviews and updates;* *(ii) the organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and* *(iii) the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan (for organization-defined frequency of contingency plan reviews and updates); other relevant documents or records.
CP-5.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records. (L) **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency plan review and update responsibilities; organizational personnel with mission-related and operational responsibilities. (L)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-6 ALTERNATE STORAGE SITE Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies an alternate storage site; and* *(ii) alternate storage site agreements are currently in place (if needed) to permit storage of information system backup information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.
CP-6.2	**ASSESSMENT OBJECTIVE:** *Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information consistent with the organization's recovery time objectives and recovery point objectives.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with alternate storage site responsibilities. (M)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-6 ALTERNATE STORAGE SITE Control Enhancement: **(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.**
CP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary storage site hazards; and* *(ii) the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.
	CP-6 ALTERNATE STORAGE SITE Control Enhancement: **(2) The organization configures the alternate storage site to facilitate timely and effective recovery operations.**
CP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate storage site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreements.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-6 ALTERNATE STORAGE SITE Control Enhancement: **(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.**
CP-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and* *(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-7 ALTERNATE PROCESSING SITE Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable. Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
CP-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies an alternate processing site;* *(ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and* *(iii) alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan (for organization-defined time period within which processing must be resumed at the alternate processing site); other relevant documents or records.
CP-7.2	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with alternate processing site responsibilities. (M)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-7 ALTERNATE PROCESSING SITE Control Enhancement: **(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.**
CP-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary processing site hazards; and* *(ii) the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.
	CP-7 ALTERNATE PROCESSING SITE Control Enhancement: **(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.**
CP-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and* *(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-7 ALTERNATE PROCESSING SITE Control Enhancement: **(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.**
CP-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records.
	CP-7 ALTERNATE PROCESSING SITE Control Enhancement: **(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.**
CP-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if alternate processing site agreements specify the requirements needed to support the minimum required operational capability of the organization.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records.
CP-7(4).2	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system at the alternate processing site.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-8 TELECOMMUNICATIONS SERVICES Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).
CP-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies primary and alternate telecommunications services to support the information system;* *(ii) the organization defines the time period within which resumption of information system operations must take place; and* *(iii) alternate telecommunications service agreements are in place to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan (for organization-defined time period within which resumption of information system operations must take place); primary and alternate telecommunications service agreements; other relevant documents or records.
CP-8.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) telecommunications services supporting the organization are used for national security emergency preparedness; and* *(ii) a common carrier provides telecommunications services.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-8 TELECOMMUNICATIONS SERVICES Control Enhancement: **(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.**
CP-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements defined in the organization's contingency plan.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.
	CP-8 TELECOMMUNICATIONS SERVICES Control Enhancement: **(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.**
CP-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if primary and alternate telecommunications services share a single point of failure.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-8 TELECOMMUNICATIONS SERVICES Control Enhancement: **(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.**
CP-8(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate telecommunications service provider's site is sufficiently separated from the primary telecommunications service provider's site so as not to be susceptible to the same hazards identified at the primary site.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.
	CP-8 TELECOMMUNICATIONS SERVICES Control Enhancement: **(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.**
CP-8(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the contingency plans for the primary and alternate telecommunications service providers are sufficient to meet the needs of the organization.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers. **Test** (DEPTH, COVERAGE): Operational capability by exercising priority-of-service provisions of alternate telecommunications service agreements.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-9 INFORMATION SYSTEM BACKUP Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location. Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.
CP-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information systems backups;* *(ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and* *(iii) the organization identifies the location(s) for storing backup information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.
CP-9.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; and* *(ii) the organization stores the backup information in designated locations in accordance with information system backup procedures.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-9 INFORMATION SYSTEM BACKUP Control Enhancement: **(1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.**
CP-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system backup testing;* *(ii) the organization conducts information system backup testing within the organization-defined frequency; and* *(iii) testing results verify backup media reliability and information integrity.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for testing backup information); information system backup test results; backup storage location(s); other relevant documents or records.
	CP-9 INFORMATION SYSTEM BACKUP Control Enhancement: **(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.**
CP-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing; and* *(ii) the use of the backup information contributes to a successful restoration of the identified functions within the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; other relevant documents or records.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-9 INFORMATION SYSTEM BACKUP Control Enhancement: **(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.**
CP-9(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization stores backup copies of operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); other relevant documents or records.
	CP-9 INFORMATION SYSTEM BACKUP Control Enhancement: **(4) The organization protects system backup information from unauthorized modification.** Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.
CP-9(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system backup responsibilities.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
CP-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
CP-10.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system recovery and reconstitution operations. (L)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control Enhancement: **(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.**
CP-10(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; contingency plan test results; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency testing responsibilities.

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents identification and authentication policy and procedures;* *(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and* *(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with identification and authentication responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
IA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with identification and authentication responsibilities. (L) (M)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST Special Publication 800-63 level 1 compliant. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST Special Publication 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals. Related security controls: AC-14, AC-17. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
IA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and* *(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST Special Publication 800-63.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing identification and authentication capability for the information system. (L)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: **(1) The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.**
IA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and* *(ii) the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device, or level 4.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system security plan (for organization-selected authentication levels); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: **(2) The information system employs multifactor authentication for *local* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3 or level 4*] compliant.**
IA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and* *(ii) the information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3 or level 4.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system security plan (for organization-selected authentication levels); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: **(3) The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 level 4 compliant.**
IA-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and* *(ii) the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION Control: The information system identifies and authenticates specific devices before establishing a connection. Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and;* *(ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing device identification and authentication. (M)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-4 IDENTIFIER MANAGEMENT Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers. Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
IA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages user identifiers by uniquely identifying each user;* *(ii) the organization manages user identifiers by verifying the identity of each user;* *(iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;* *(iv) the organization manages user identifiers by issuing the identifier to the intended party;* *(v) the organization defines the time period of inactivity after which a user identifier is to be disabled;* *(vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and* *(vii) the organization manages user identifiers by archiving identifiers.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. **Test** (DEPTH, COVERAGE): Identity verification capability for the information system and for organizational facilities. (L)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
IA-4.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses a personal identity verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. **Test** (DEPTH, COVERAGE): Identity verification capability for the information system and for organizational facilities. (L)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
IA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages information system authenticators by defining initial authenticator content;* *(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;* *(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and* *(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing authenticator management functions. (L)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-6 AUTHENTICATOR FEEDBACK Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
IA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing authenticator feedback. (L)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
IA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing cryptographic module authentication. (L)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. Supplemental Guidance: The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents incident response policy and procedures;* *(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review incident response policy and procedures; and* *(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response planning and plan implementation responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
IR-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response planning and plan implementation responsibilities. (L) (M)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-2 INCIDENT RESPONSE TRAINING Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*]. Supplemental Guidance: None.
IR-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies and documents personnel with incident response roles and responsibilities;* *(ii) the organization provides incident response training to personnel with incident response roles and responsibilities;* *(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;* *(iv) the organization defines the frequency of refresher incident response training; and* *(v) the organization provides refresher incident response training in accordance with organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response training; incident response training material; information system security plan (for organization-defined frequency for refresher incident response training); incident response training records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response training and operational responsibilities.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-2 INCIDENT RESPONSE TRAINING Control Enhancement: **(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.**
IR-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response training and operational responsibilities.
	IR-2 INCIDENT RESPONSE TRAINING Control Enhancement: **(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.**
IR-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environment.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms supporting incident response training; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response training and operational responsibilities. **Test** (DEPTH, COVERAGE): Simulated incident response training events.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-3 INCIDENT RESPONSE TESTING AND EXERCISES Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results. Supplemental Guidance: NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.
IR-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines incident response tests/exercises;* *(ii) the organization defines the frequency of incident response tests/exercises;* *(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and* *(iv) the organization documents the results of incident response tests/exercises.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of organization-defined tests/exercises and organization-defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant documents or records.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-3 INCIDENT RESPONSE TESTING AND EXERCISES Control Enhancement: **(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.** Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.
IR-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system; and* *(ii) the automated mechanisms supporting incident response testing provide more complete coverage of incident response issues, more realistic test/exercise scenarios, and a greater stress on the incident response capability.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of organization-defined tests/exercises); incident response testing documentation; automated mechanisms supporting incident response tests/exercises; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response testing responsibilities.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-4 INCIDENT HANDLING Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Related security controls: AU-6, PE-6. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and* *(ii) the incident handling capability is consistent with NIST Special Publication 800-61.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident handling capability; NIST Special Publication 800-61; other relevant documents or records. **Test** (DEPTH, COVERAGE): Incident handling capability for the organization. (L) (M) **Interview** (DEPTH, COVERAGE): Organizational personnel with incident handling responsibilities. (L)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-4 INCIDENT HANDLING Control Enhancement: **(1) The organization employs automated mechanisms to support the incident handling process.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to support the incident handling process.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident handling capability; automated mechanisms supporting incident handling; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident handling responsibilities. (M)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-5 INCIDENT MONITORING Control: The organization tracks and documents information system security incidents on an ongoing basis. Supplemental Guidance: None. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks and documents information system security incidents on an ongoing basis.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident monitoring capability; incident response records and documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Incident monitoring capability for the organization. (M) **Interview** (DEPTH, COVERAGE): Organizational personnel with incident monitoring responsibilities. (M)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-5 INCIDENT MONITORING Control Enhancement: **(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.**
IR-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident monitoring responsibilities.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-6 INCIDENT REPORTING Control: The organization promptly reports incident information to appropriate authorities. Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST Special Publication 800-61 provides guidance on incident reporting. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization promptly reports incident information to appropriate authorities;* *(ii) incident reporting is consistent with NIST Special Publication 800-61.* (L) *(iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and* *(iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident reporting; NIST Special Publication 800-61; incident reporting records and documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident reporting responsibilities. (L) **Test** (DEPTH, COVERAGE): Incident reporting capability for the organization. (L) (M)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-6 INCIDENT REPORTING Control Enhancement: **(1) The organization employs automated mechanisms to assist in the reporting of security incidents.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident reporting responsibilities. (M)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-7 INCIDENT RESPONSE ASSISTANCE Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability. Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
IR-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and* *(ii) the incident response support resource is an integral part of the organization's incident response capability.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response assistance; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response assistance and support responsibilities. (L)

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	IR-7 INCIDENT RESPONSE ASSISTANCE Control Enhancement: **(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
IR-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance. (M)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
MA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents information system maintenance policy and procedures;* *(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and* *(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
MA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities. (L) (M)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-2 CONTROLLED MAINTENANCE Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. Supplemental Guidance: All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
MA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities. (L)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-2 CONTROLLED MAINTENANCE Control Enhancement: **(1) The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).**
MA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records.
	MA-2 CONTROLLED MAINTENANCE Control Enhancement: **(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.**
MA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to schedule and conduct maintenance as required, and to create accurate, complete, and available records of all maintenance actions, both needed and completed.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-3 MAINTENANCE TOOLS Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis. Supplemental Guidance: The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.
MA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization approves, controls, and monitors the use of information system maintenance tools; and* *(ii) the organization maintains maintenance tools on an ongoing basis.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-3 MAINTENANCE TOOLS Control Enhancement: **(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.** Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.
MA-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities.
	MA-3 MAINTENANCE TOOLS Control Enhancement: **(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.**
MA-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization checks all media containing diagnostic test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-3 MAINTENANCE TOOLS Control Enhancement: **(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.**
MA-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization either checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; and* *(ii) the organization retains the maintenance equipment within the facility or destroys the equipment if the equipment cannot be sanitized, unless an appropriate organization official explicitly authorizes an exception.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities.
	MA-3 MAINTENANCE TOOLS Control Enhancement: **(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.**
MA-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting information system maintenance activities.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-4 REMOTE MAINTENANCE Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed. Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm. Related security controls: IA-2, MP-6. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
MA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities. (L)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-4 REMOTE MAINTENANCE Control Enhancement: **(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.**
MA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization audits all remote maintenance and diagnostic sessions; and* *(ii) designated organizational personnel review the maintenance records of remote sessions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing remote maintenance for the information system; maintenance records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities.
	MA-4 REMOTE MAINTENANCE Control Enhancement: **(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.**
MA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing remote maintenance for the information system; information system security plan; maintenance records; audit records; other relevant documents or records.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-4 REMOTE MAINTENANCE Control Enhancement: **(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.**
MA-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization does not allow remote diagnostic or maintenance services to be performed by a provider that does not implement for its own information system, a level of security at least as high as the level of security implemented on the information system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing remote maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities; information system maintenance provider.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-5 MAINTENANCE PERSONNEL Control: The organization allows only authorized personnel to perform maintenance on the information system. Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
MA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization allows only authorized personnel perform maintenance on the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities. (L)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MA-6 TIMELY MAINTENANCE Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure. Supplemental Guidance: None.
MA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines key information system components;* *(ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and* *(iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system maintenance responsibilities.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
MP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents media protection policy and procedures;* *(ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review media protection policy and procedures; and* *(iv) the organization updates media protection policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Media protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media protection responsibilities. (L) (M)
MP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Media protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media protection responsibilities. (L) (M)

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-2 MEDIA ACCESS Control: The organization restricts access to information system media to authorized individuals. Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
MP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts access to information system media to authorized users.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media protection responsibilities. (L)

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-2 MEDIA ACCESS Control Enhancement: **(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.** Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices). (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
MP-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to restrict access to media storage areas; and* *(ii) the organization employs automated mechanisms to audit access attempts and access granted.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access restrictions to media storage areas. (M)

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-3 MEDIA LABELING Control: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [*Assignment: organization-defined list of media types or hardware components*] from labeling so long as they remain within [*Assignment: organization-defined protected environment*]. Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.
MP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines its protected environment for media labeling requirements;* *(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;* *(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and* *(iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan (for list of organization-defined media types and hardware components exempted from external labeling requirements and for organization's definition of protected environment for the organization); removable storage media and information system output; other relevant documents or records.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-4 MEDIA STORAGE Control: The organization physically controls and securely stores information system media within controlled areas. Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures. As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Related security controls: CP-9, RA-2.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
MP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines controlled areas for information system media;* *(ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;* *(iii) the organization defines the specific measures used to protect the selected media and information contained on that media;* *(iv) the organization physically controls and securely stores information system media within controlled areas; and* *(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for the definition of controlled areas for the organization); information system media; other relevant documents or records.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-5 MEDIA TRANSPORT Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).
MP-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel authorized to transport information system media outside of controlled areas;* *(ii) the organization controls information system media during transport outside of controlled areas; and* *(iii) the organization restricts the activities associated with transport of information system media to authorized personnel.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for definition of controlled areas for the organization); list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-5 MEDIA TRANSPORT Control Enhancement: **(1) The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*].** Enhancement Supplemental Guidance: Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
MP-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas;* *(ii) the organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for the definition of controlled areas for the organization); information system media transport records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media transport responsibilities. (M)

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-5 MEDIA TRANSPORT Control Enhancement: **(2) The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].** Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.
MP-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a system of records for documenting activities associated with the transport of information system media; and* *(ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for organization-defined system of records for media transport); information system media transport records; audit records; other relevant documents or records.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-5 MEDIA TRANSPORT Control Enhancement: **(3) The organization employs an identified custodian at all times to transport information system media.** Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.
MP-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an identified custodian at all times to transport information system media.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media transport responsibilities.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-6 MEDIA SANITIZATION AND DISPOSAL Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse. Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
MP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;* *(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and* *(iii) information system media sanitation is consistent with NIST Special Publication 800-88.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media sanitization and disposal; NIST Special Publication 800-88; media sanitization records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media sanitization responsibilities. (L)

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	MP-6 MEDIA SANITIZATION AND DISPOSAL Control Enhancement: **(1) The organization tracks, documents, and verifies media sanitization and disposal actions.**
MP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media sanitization responsibilities. [*Note: Compare organizational personnel descriptions of information system media sanitization activities with established organizational policy and procedures.*]
	MP-6 MEDIA SANITIZATION AND DISPOSAL Control Enhancement: **(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.**
MP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization periodically tests sanitization equipment and procedures to verify correct performance.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system media sanitization responsibilities.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
PE-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents physical and environmental protection policy and procedures;* *(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and* *(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with physical and environmental protection responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
PE-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with physical and environmental protection responsibilities. (L) (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-2 PHYSICAL ACCESS AUTHORIZATIONS Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*]. Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.
PE-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies areas within the facility that are publicly accessible;* *(ii) the organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility;* *(iii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);* *(iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and* *(v) designated officials within the organization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-3 PHYSICAL ACCESS CONTROL Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76. (L) Indicates that this section of the assessment procedure is optional for low-impact systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);* *(ii) the organization verifies individual access authorizations before granting access to the facility; and* *(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Physical access control capability. (L) **Interview** (DEPTH, COVERAGE): Organizational personnel with physical access control responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
PE-3.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis;* *(ii) the organization secures keys, combinations and other access devices on a regular basis; and* *(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records. **Test** (DEPTH, COVERAGE): Physical access control devices. (L)
PE-3.3	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the access control system is consistent with FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);* *(ii) the access control system is consistent with NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and* *(iii) the access control system is consistent with NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Physical access control devices. (L)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-3 PHYSICAL ACCESS CONTROL Control Enhancement: **(1) The organization controls physical access to the information system independent of the physical access controls for the facility.** Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.
PE-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies specific areas within the facility containing large concentrations of information system components or components requiring additional physical protection; and* *(ii) for an information system identified as requiring additional physical protection or part of a large concentration of information system components, the organization controls physical access to the system independent of the physical access controls for the facility.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities. Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.
PE-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. Supplemental Guidance: None.
PE-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-6 MONITORING PHYSICAL ACCESS Control: The organization monitors physical access to the information system to detect and respond to physical security incidents. Supplemental Guidance: The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability. (L) Indicates that this section of the assessment procedure is optional for low-impact systems.
PE-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Physical access monitoring capability. (L) **Interview** (DEPTH, COVERAGE): Organizational personnel with physical access monitoring responsibilities. (L)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-6 MONITORING PHYSICAL ACCESS Control Enhancement: **(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
PE-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization monitors real-time intrusion alarms and surveillance equipment.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with physical access monitoring responsibilities. (M)
	PE-6 MONITORING PHYSICAL ACCESS Control Enhancement: **(2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.**
PE-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing physical access monitoring capability.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-7 VISITOR CONTROL Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79. (L) Indicates that this section of the assessment procedure is optional for low-impact systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Visitor access control capability. (L) **Interview** (DEPTH, COVERAGE): Organizational personnel with visitor access control responsibilities. (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-7 VISITOR CONTROL Control Enhancement: **(1) The organization escorts visitors and monitors visitor activity, when required.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization escorts visitors and monitors visitor activity, when required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with visitor access control responsibilities. (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-8 ACCESS RECORDS Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency*]. Supplemental Guidance: None.
PE-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of review for visitor access records;* *(ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:* - *name and organization of the person visiting;* - *signature of the visitor;* - *form of identification;* - *date of access;* - *time of entry and departure;* - *purpose of visit;* - *name and organization of person visited and* *(iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records); facility access control records; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-8 ACCESS RECORDS Control Enhancement: **(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.**
PE-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine the organization employs automated mechanisms to facilitate the maintenance and review of access records.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; other relevant documents or records.
	PE-8 ACCESS RECORDS Control Enhancement: **(2) The organization maintains a record of all physical access, both visitor and authorized individuals.**
PE-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-9 POWER EQUIPMENT AND POWER CABLING Control: The organization protects power equipment and power cabling for the information system from damage and destruction. Supplemental Guidance: None.
PE-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-9 POWER EQUIPMENT AND POWER CABLING Control Enhancement: **(1) The organization employs redundant and parallel power cabling paths.**
PE-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs redundant and parallel power cabling paths.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-10 EMERGENCY SHUTOFF Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.
PE-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms); and* *(ii) the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-10 EMERGENCY SHUTOFF Control Enhancement: **(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.**
PE-10(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the emergency power-off capability from accidental or unauthorized activation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-11 EMERGENCY POWER Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. Supplemental Guidance: None. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
PE-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Uninterruptible power supply. (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-11 EMERGENCY POWER Control Enhancement: **(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.**
PE-11(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Alternate power supply.
	PE-11 EMERGENCY POWER Control Enhancement: **(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.**
PE-11(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Alternate power supply.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-12 EMERGENCY LIGHTING Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes. Supplemental Guidance: None. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PE-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and* *(ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records. **Test** (DEPTH, COVERAGE): Emergency lighting capability. (L)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-13 FIRE PROTECTION Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.
PE-13.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-13 FIRE PROTECTION Control Enhancement: **(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs fire detection devices/systems that activate automatically; and* *(ii) the organization employs fire detection devices/systems that notify the organization and emergency responders in the event of a fire.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Simulated fire detection and automated notifications. (M)
	PE-13 FIRE PROTECTION Control Enhancement: **(2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-13(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records. **Test** (DEPTH, COVERAGE): Simulated fire detection and automated notifications. (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-13 FIRE PROTECTION Control Enhancement: **(3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact systems and below.
PE-13(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records. **Test** (DEPTH, COVERAGE): Simulated fire detection and automated notifications. (M)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-14 TEMPERATURE AND HUMIDITY CONTROLS Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides. Supplemental Guidance: None.
PE-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and* *(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-15 WATER DAMAGE PROTECTION Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. Supplemental Guidance: None. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PE-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system; and* *(ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Simulated master water shutoff value activation for the plumbing system. (L) **Interview** (DEPTH, COVERAGE): Organization personnel with physical and environmental protection responsibilities. (L)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-15 WATER DAMAGE PROTECTION Control Enhancement: **(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.**
PE-15(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing master water shutoff valve activation.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-16 DELIVERY AND REMOVAL Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items. Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PE-16.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; and* *(ii) the organization maintains appropriate records of items entering and exiting the facility.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organization personnel with tracking responsibilities for information system components entering and exiting the facility. (L)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-17 ALTERNATE WORK SITE Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites. Supplemental Guidance: The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications.
PE-17.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organization personnel using alternate work sites.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.
PE-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and* *(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS Control Enhancement: **(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.**
PE-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards; and* *(ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organization personnel with site selection responsibilities for the facility housing the information system.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PE-19 INFORMATION LEAKAGE Control: The organization protects the information system from information leakage due to electromagnetic signals emanations. Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.
PE-19.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the information system from information leakage due to electromagnetic signals emanations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms protecting the information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system for information leakage due to electromagnetic signals emanations.

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-1 SECURITY PLANNING POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
PL-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents security planning policy and procedures;* *(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review security planning policy and procedures; and* *(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security planning and plan implementation responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
PL-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security planning and plan implementation responsibilities. (L) (M)

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-2 SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan. Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PL-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and implements a security plan for the information system;* *(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;* *(iii) the security plan is consistent with NIST Special Publication 800-18;* (L) *(iv) the security plan is consistent with the organization's information system architecture and information security architecture; and* *(v) designated organizational officials review and approve the security plan.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy; procedures addressing information system security plan development and implementation; NIST Special Publication 800-18; security plan for the information system; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security planning and plan implementation responsibilities. (L)

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-3 SYSTEM SECURITY PLAN UPDATE Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments. Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PL-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system security plan reviews and updates;* *(ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually;* *(iii) the organization receives input to update the security plan from the organization's configuration management and control process;* (L) *and* *(iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy; procedures addressing information system security plan reviews and updates; information system security plan (for organization-defined frequency for security plan updates); configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records.

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-4 RULES OF BEHAVIOR Control: The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PL-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;* *(ii) the organization makes the rules available to all information system users;* *(iii) the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18;* (L) *and* *(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST Special Publication 800-18; rules of behavior; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel who are authorized users of the information system and have signed rules of behavior. (L)

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-5 PRIVACY IMPACT ASSESSMENT Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy. Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.
PL-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts a privacy impact assessment on the information system in accordance with OMB policy; and* *(ii) the privacy impact assessment is consistent with federal legislation and OMB policy.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy; procedures for conducting privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.

FAMILY: PLANNING **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PL-6 SECURITY-RELATED ACTIVITY PLANNING Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.
PL-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and* *(ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Security planning policy; procedures for planning security-related activities for the information system; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security planning and plan implementation responsibilities.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
PS-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents personnel security policy and procedures;* *(ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review personnel security policy and procedures; and* *(iv) the organization updates personnel security policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy and procedures, other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with personnel security responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
PS-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with personnel security responsibilities. (L) (M)

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-2 POSITION CATEGORIZATION Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*]. Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.
PS-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns a risk designations to all positions within the organization;* *(ii) the organization establishes a screening criteria for individuals filling organizational positions;* *(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;* *(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and* *(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan (for organization-defined frequency for review of position categorizations); records of risk designation reviews and updates; other relevant documents or records.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-3 PERSONNEL SCREENING Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access. Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.
PS-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and* *(ii) the personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures for personnel screening; records of screened personnel; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; other relevant documents or records.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-4 PERSONNEL TERMINATION Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems. Supplemental Guidance: Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PS-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization terminates information system access upon termination of individual employment;* *(ii) the organization conducts exit interviews of terminated personnel;* *(iii) the organization retrieves all organizational information system-related property from terminated personnel; and* *(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with personnel security responsibilities. (L)

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-5 PERSONNEL TRANSFER Control: The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).
PS-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and* *(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-6 ACCESS AGREEMENTS Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*]. Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.
PS-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;* *(ii) organizational personnel sign access agreements;* *(iii) the organization defines the frequency of reviews and updates for access agreements; and* *(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-7 THIRD-PARTY PERSONNEL SECURITY Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance. Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
PS-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management);* *(ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35; and* *(iii) the organization monitors third-party provider compliance with personnel security requirements.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with personnel security responsibilities; third-party providers. (L)

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	PS-8 PERSONNEL SANCTIONS Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.
PS-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and* *(ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-1 RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
RA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents risk assessment policy and procedures;* *(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review risk assessment policy and procedures; and* *(iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with risk assessment responsibilities. (L) (M)
RA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with risk assessment responsibilities. (L) (M)

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-2 SECURITY CATEGORIZATION Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations. Supplemental Guidance: The applicable federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related security controls: MP-4, SC-7. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
RA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts the security categorization of the information system as an enterprise-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;* *(ii) the security categorization is consistent with FIPS 199 and NIST Special Publication 800-60;* *(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;* *(iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and* *(v) designated, senior-level organizational officials review and approve the security categorization of the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST Special Publication 800-60; information system security plan; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security categorization and risk assessment responsibilities. (L)

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-3 RISK ASSESSMENT Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties). Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
RA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and* *(ii) the risk assessment is consistent with the NIST Special Publication 800-30.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST Special Publication 800-30; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with risk assessment responsibilities. (L)

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-4 RISK ASSESSMENT UPDATE Control: The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system. Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
RA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of risk assessment updates;* *(ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;* *(iii) the risk assessment update is consistent with the NIST Special Publications 800-30;* (L) *and* *(iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST Special Publication 800-30; other relevant documents or records.

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-5 VULNERABILITY SCANNING Control: The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities potentially affecting the system are identified and reported. Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
RA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of vulnerability scans within the information system;* *(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported;* *(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact;* *(iv) the organization performs network vulnerability scanning in accordance with NIST Special Publication 800-42; and* *(v) the organization handles patch and vulnerability management in accordance with NIST Special Publication 800-40.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with risk assessment and vulnerability scanning responsibilities. (M)

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-5 VULNERABILITY SCANNING Control Enhancement: **(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.**
RA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned; and* *(ii) the vulnerability scanning tools retrieve updated lists of information system vulnerabilities from the National Vulnerability Database (NVD).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Vulnerability scanning capability and associated scanning tools.
	RA-5 VULNERABILITY SCANNING Control Enhancement: **(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when significant new vulnerabilities are identified and reported.**
RA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of updates for information system vulnerabilities scanned; and* *(ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when significant new vulnerabilities are identified and reported.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for updates to list of vulnerabilities to be scanned); list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records.

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	RA-5 VULNERABILITY SCANNING Control Enhancement: **(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.**
RA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements procedures that can demonstrate the breadth of scan coverage (including information system components scanned); and* *(ii) the organization implements procedures that can demonstrate the depth of scan coverage (including vulnerabilities checked).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(v) the organization develops and documents system and services acquisition policy and procedures;* *(i) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;* *(ii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and* *(iii) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and services acquisition responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
SA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and services acquisition responsibilities. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-2 ALLOCATION OF RESOURCES Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system. Supplemental Guidance: The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;* *(ii) the organization determines security requirements for the information system in mission/business case planning;* *(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and* *(iv) the organization's programming and budgeting process is consistent with NIST Special Publication 800-65.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST Special Publication 800-65; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with capital planning and investment responsibilities. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-3 LIFE CYCLE SUPPORT Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations. Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and* *(ii) the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information security and system life cycle development responsibilities. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-4 ACQUISITIONS Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Supplemental Guidance: *Solicitation Documents* The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. *Information System Documentation* The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system. *Use of Tested, Evaluated, and Validated Products* NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products. *Configuration Settings and Implementation Guidance* The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
SA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards;* *(ii) the organization's acquisition of commercial information technology products is consistent with NIST Special Publication 800-23;* (L) *(iii) references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST Special Publication 800-70;* (L) *and* *(iv) acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe:* - *required security capabilities;* - *required design and development processes;* - *required test and evaluation procedures; and* - *required documentation.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST Special Publications 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security, acquisition, and contracting responsibilities. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-4 ACQUISITIONS Control Enhancement: **(1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.**
SA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security, acquisition, and contracting responsibilities.
	SA-4 ACQUISITIONS Control Enhancement: **(2) The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).**
SA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security, acquisition, and contracting responsibilities.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;* *(ii) the organization makes available information on configuring, installing, and operating the information system;* (L) *and* *(iii) the organization makes available information on effectively using the security features in the information system.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-5 INFORMATION SYSTEM DOCUMENTATION Control Enhancement: **(1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.**
SA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the requirements for information system documentation; information system design documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.
	SA-5 INFORMATION SYSTEM DOCUMENTATION Control Enhancement: **(2) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).**
SA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing the requirements for information system documentation; information system design documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-6 SOFTWARE USAGE RESTRICTIONS Control: The organization complies with software usage restrictions. Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization complies with software usage restrictions; and* *(ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-7 USER INSTALLED SOFTWARE Control: The organization enforces explicit rules governing the installation of software by users. Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect). (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization enforces explicit rules governing the installation of software by users;* *(ii) unauthorized software is present on the system;* (L) *and* *(iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. (L) **Test** (DEPTH, COVERAGE): Enforcement of rules for user installed software on the information system; information system for prohibited software. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-8 SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SA-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization designs and implements the information system using security engineering principles; and* *(ii) the organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST Special Publication 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and services acquisition responsibilities. (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-9 EXTERNAL INFORMATION SYSTEM SERVICES Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance. Supplemental Guidance: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
SA-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;* *(ii) the organization monitors security control compliance;* *(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions;* (L) *and* *(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and services acquisition responsibilities; external providers of information system services. (L) (M)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-10 DEVELOPER CONFIGURATION MANAGEMENT Control: The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation. Supplemental Guidance: This control also applies to the development actions associated with information system changes.
SA-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SA-11 DEVELOPER SECURITY TESTING Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results. Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.
SA-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents system and communications protection policy and procedures;* *(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and* *(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and communications protection responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
SC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and communications protection responsibilities. (L) (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-2 APPLICATION PARTITIONING Control: The information system separates user functionality (including user interface services) from information system management functionality. Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system separates user functionality (including user interface services) from information system management functionality.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Separation of user functionality from information system management functionality. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-3 SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from nonsecurity functions. Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.
SC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and* *(ii) the information system isolates security functions from nonsecurity functions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Separation of security functions from nonsecurity functions within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-3 SECURITY FUNCTION ISOLATION Control Enhancement: **(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.**
SC-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs underlying hardware separation mechanisms to facilitate security function isolation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Hardware separation mechanisms facilitating security function isolation.
	SC-3 SECURITY FUNCTION ISOLATION Control Enhancement: **(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.**
SC-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the critical security functions of the information system to be isolated from both nonsecurity functions and from other security functions; and* *(ii) the information system isolates critical security functions from both nonsecurity functions and from other security functions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Isolation of critical security functions.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-3 SECURITY FUNCTION ISOLATION Control Enhancement: **(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.**
SC-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
	SC-3 SECURITY FUNCTION ISOLATION Control Enhancement: **(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.**
SC-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-3 SECURITY FUNCTION ISOLATION Control Enhancement: **(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.**
SC-3(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-4 INFORMATION REMNANCE Control: The information system prevents unauthorized and unintended information transfer via shared system resources. Supplemental Guidance: Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system for unauthorized and unintended transfer of information via shared system resources. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-5 DENIAL OF SERVICE PROTECTION Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*]. Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and* *(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system for protection against or limitation of the effects of denial of service attacks. (L) (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-5 DENIAL OF SERVICE PROTECTION Control Enhancement: **(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.**
SC-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system for protection against or limitation of the effects of denial of service attacks.
	SC-5 DENIAL OF SERVICE PROTECTION Control Enhancement: **(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.**
SC-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-6 RESOURCE PRIORITY Control: The information system limits the use of resources by priority. Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.
SC-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system limits the use of resources by priority.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-7 BOUNDARY PROTECTION Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning. The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks. Related security controls: MP-4, RA-2. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines key internal boundaries of the information system; and* *(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Selected organizational personnel with boundary protection responsibilities. (L) **Test** (DEPTH, COVERAGE): Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system. (L) (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.** Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.
SC-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the mediation necessary for public access to the organization's internal networks; and* *(ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access controls for public access to the organization's internal networks. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.**
SC-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service; and* *(ii) the organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Selected organizational personnel with boundary protection responsibilities. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).** (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-7(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system denies network traffic by default and allows network traffic by exception.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Selected organizational personnel with boundary protection responsibilities. (M)
	SC-7 BOUNDARY PROTECTION Control Enhancement: **(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.**
SC-7(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting the fail-safe boundary protection capability within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-8 TRANSMISSION INTEGRITY Control: The information system protects the integrity of transmitted information. Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity of transmitted information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Transmission integrity capability within the information system. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-8 TRANSMISSION INTEGRITY Control Enhancement: **(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.** Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.
SC-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Cryptographic mechanisms implementing transmission integrity capability within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-9 TRANSMISSION CONFIDENTIALITY Control: The information system protects the confidentiality of transmitted information. Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related security control: AC-17. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the confidentiality of transmitted information.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Transmission confidentiality capability within the information system. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-9 TRANSMISSION CONFIDENTIALITY Control Enhancement: **(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.** Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.
SC-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Cryptographic mechanisms implementing transmission confidentiality capability within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-10 NETWORK DISCONNECT Control: The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity. Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements.
SC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of inactivity before the information system terminates a network connection; and* *(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Network disconnect capability within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-11 TRUSTED PATH Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*]. Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).
SC-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions within the information system that are included in a trusted communications path;* *(ii) the organization-defined security functions include information system authentication and reauthentication; and* *(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing trusted communications paths; information system security plan (for organization-defined security functions to include for authentication and reauthentication); information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing trusted communications paths within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-12.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with responsibilities for cryptographic key establishment or management. (M) **Test** (DEPTH, COVERAGE): Automated mechanisms implementing cryptographic key management and establishment within the information system. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-13 USE OF CRYPTOGRAPHY Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Supplemental Guidance: The applicable federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.
SC-13.1	**ASSESSMENT OBJECTIVE:** *Determine if, for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-14 PUBLIC ACCESS PROTECTIONS Control: The information system protects the integrity and availability of publicly available information and applications. Supplemental Guidance: None. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity and availability of publicly available information and applications.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system. (L) (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-15 COLLABORATIVE COMPUTING Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. Supplemental Guidance: Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-15.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-15 COLLABORATIVE COMPUTING Control Enhancement: **(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.**
SC-15(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides physical disconnect of camera and microphone in a manner that supports ease of use.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Physical disconnect of collaborative computing devices.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-16 TRANSMISSION OF SECURITY PARAMETERS Control: The information system reliably associates security parameters with information exchanged between information systems. Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.
SC-16.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system reliably associates security parameters with information exchanged between information systems.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting reliable transmission of security parameters between information systems.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. Supplemental Guidance: For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST Special Publication 800-32; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with public key infrastructure certificate issuing responsibilities. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-18 MOBILE CODE Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system. Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and* *(ii) the organization authorizes, monitors, and controls the use of mobile code within the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST Special Publication 800-28; other relevant documents or records. **Test** (DEPTH, COVERAGE): Mobile code authorization and monitoring capability for the organization. (M) **Interview** (DEPTH, COVERAGE): Organizational personnel with mobile code authorization, monitoring, and control responsibilities. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-19 VOICE OVER INTERNET PROTOCOL Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system. Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and* *(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing VoIP; NIST Special Publication 800-58; VoIP usage restrictions; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with VoIP authorization and monitoring responsibilities. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) Control Enhancement: **(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.** Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.
SC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems. Supplemental Guidance: A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.
SC-21.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing data origin authentication and integrity verification for resolution services within the information system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) Control Enhancement: **(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.** Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.
SC-21(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system performs data origin authentication and data integrity verification on all resolution response received whether or not client systems explicitly request this service.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation. Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST Special Publication 800-81 provides guidance on secure DNS deployment. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-22.1	**ASSESSMENT OBJECTIVE:** *Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); access control policy and procedures; NIST Special Publication 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting name/address resolution service for fault tolerance and role separation. (M)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SC-23 SESSION AUTHENTICITY Control: The information system provides mechanisms to protect the authenticity of communications sessions. Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SC-23.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides mechanisms to protect the authenticity of communications sessions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and communications protection policy; procedures addressing session authenticity; NIST Special Publications 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing session authenticity. (M)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SI-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents system and information integrity policy and procedures;* *(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;* *(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and* *(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and information integrity responsibilities. (L) (M)

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
SI-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* *(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;* (L) *and* *(iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy and procedures; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with system and information integrity responsibilities. (L) (M)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-2 FLAW REMEDIATION Control: The organization identifies, reports, and corrects information system flaws. Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST Special Publication 800-40, provides guidance on security patch installation and patch management. Related security controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
SI-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies, reports, and corrects information system flaws;* *(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;* (L) *(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;* (L) *(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation;* (L) *and* *(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with flaw remediation responsibilities. (L)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-2 FLAW REMEDIATION Control Enhancement: **(1) The organization centrally manages the flaw remediation process and installs updates automatically.**
SI-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages the flaw remediation process and installs updates automatically.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.
	SI-2 FLAW REMEDIATION Control Enhancement: **(2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.**
SI-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing information system flaw remediation update status.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-3 MALICIOUS CODE PROTECTION Control: The information system implements malicious code protection. Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST Special Publication 800-83 provides guidance on implementing malicious code protection.
SI-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system implements malicious code protection;* *(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;* *(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;* *(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and* *(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing malicious code protection; NIST Special Publication 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-3 MALICIOUS CODE PROTECTION Control Enhancement: **(1) The organization centrally manages malicious code protection mechanisms.**
SI-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages malicious code protection mechanisms.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.
	SI-3 MALICIOUS CODE PROTECTION Control Enhancement: **(2) The information system automatically updates malicious code protection mechanisms.**
SI-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization automatically updates malicious code protection mechanisms.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automatic update capability for malicious code protection.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8.
SI-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: **(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.**
SI-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system-wide intrusion detection capability.
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: **(2)The organization employs automated tools to support near-real-time analysis of events.**
SI-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to support near-real-time analysis of events.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated tools supporting near real-time event analysis.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: **(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.**
SI-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: **(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.** Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.
SI-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the types of activities or conditions considered unusual or unauthorized; and* *(ii) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; types of activities or conditions considered usual or unauthorized; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system monitoring capability for inbound and outbound communications.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: **(5) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].**
SI-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies indications of compromise or potential compromise to the security of the information system; and* *(ii) the information system provides a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system security plan (for organization-defined list of indicators of potential compromise to the security of the information system); information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system monitoring real-time alert capability.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-5 SECURITY ALERTS AND ADVISORIES Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. Supplemental Guidance: The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems.
SI-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization receives information system security alerts/advisories on a regular basis;* *(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and* *(iii) the organization takes appropriate actions in response to security alerts/advisories.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing security alerts and advisories; NIST Special Publication 800-40; records of security alerts and advisories; other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system. (L)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-5 SECURITY ALERTS AND ADVISORIES Control Enhancement: **(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.**
SI-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing the distribution of security alert and advisory information.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-6 SECURITY FUNCTIONALITY VERIFICATION Control: The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered. Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.
SI-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the appropriate conditions for conducting security function verification;* *(ii) the organization defines, for periodic security function verification, the frequency of the verifications;* *(iii) the organization defines information system responses to anomalies discovered during security function verification;* *(iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and* *(v) the information system responds to security function anomalies in accordance with organization-defined responses.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan (for organization-defined conditions for conducting security function verification, organization-defined frequency of security function verifications (if periodic), and organization-defined information system responses to security function anomalies); information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Security function verification capability.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-6 SECURITY FUNCTIONALITY VERIFICATION Control Enhancement: **(1) The organization employs automated mechanisms to provide notification of failed automated security tests.**
SI-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to provide notification of failed security tests.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan (for organization-defined conditions for conducting security function verification, organization-defined frequency of security function verifications (if periodic), and information system responses to security function anomalies); information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms implementing alerts and/or notifications for failed automated security tests.
	SI-6 SECURITY FUNCTIONALITY VERIFICATION Control Enhancement: **(2) The organization employs automated mechanisms to support management of distributed security testing.**
SI-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to support management of distributed security testing.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan (for organization-defined conditions for conducting security function verification, organization-defined frequency of security function verifications (if periodic), and information system responses to security function anomalies); information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automated mechanisms supporting the management of distributed security function testing.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-7 SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information. Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.
SI-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system detects and protects against unauthorized changes to software and information; and* *(ii) the organization employs effective integrity verification tools in accordance with good software engineering practices.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Software integrity protection and verification capability.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-7 SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: **(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the system.**
SI-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of integrity scans on the information system; and* *(ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing software and information integrity; information system security plan (for organization-defined frequency for integrity scans); information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.
	SI-7 SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: **(2) The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.**
SI-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-7 SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: **(3) The organization employs centrally managed integrity verification tools.**
SI-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs centrally managed integrity verification tools.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-8 SPAM PROTECTION Control: The information system implements spam protection. Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.
SI-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system implements spam protection;* *(ii) the organization employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network;* *(iii) the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and* *(iv) the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Spam detection and handling capability.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-8 SPAM PROTECTION Control Enhancement: **(1) The organization centrally manages spam protection mechanisms.**
SI-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages spam protection mechanisms.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.
	SI-8 SPAM PROTECTION Control Enhancement: **(2) The information system automatically updates spam protection mechanisms.**
SI-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system automatically updates spam protection mechanisms.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Automatic update capability for spam protection.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.
SI-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts the capability to input information to the information system to authorized personnel.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SI-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system checks information for accuracy, completeness, validity, and authenticity;* *(ii) checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible;* *(iii) the information system employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; and* *(iv) the information system prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system capability for checking information for accuracy, completeness, validity, and authenticity. (M)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-11 ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SI-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries;* *(ii) the information system reveals only essential information to authorized individuals; and* *(iii) the information system does not include sensitive information in error logs or associated administrative messages.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test** (DEPTH, COVERAGE): Information system error handling capability. (M)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

STEP NO.	SPECIALIZED ASSESSMENT PROCEDURE
	SI-12 INFORMATION OUTPUT HANDLING AND RETENTION Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Supplemental Guidance: None. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
SI-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and* *(ii) the organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE): System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records. **Interview** (DEPTH, COVERAGE): Organizational personnel with information output handling and retention responsibilities. (M)

Section II: Extended Assessment Procedure

STEP NO.	EXTENDED ASSESSMENT PROCEDURE
EAP	The following extended assessment procedure and the associated procedural steps complement the specialized assessment procedures in the catalog. The specialized assessment procedures reflect the NIST Special Publication 800-53 requirement for assurance that the specified functionality in the security control has been implemented. The extended assessment procedure reflects other important aspects of the Special Publication 800-53 assurance requirements. The extended assessment procedure is applied on an assessment by assessment basis typically according to how the organization chose to achieve the associated Special Publication 800-53 assurances for the information system under assessment. For example, the extended assessment procedure can be applied on a per control basis, a per control family basis, a per system basis, or a per organization basis. Organizations retain maximum flexibility in applying the extended assessment procedure and should describe its specific application in the security assessment plan. (L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.
EAP.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization has a process in place to address in a timely manner, any flaws discovered in the implementation or application of the security controls in the information system.* **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE):* Policies, procedures, records, documents, activities, or mechanisms related to addressing flaws in security controls or control enhancements. * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.
EAP.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization has a process in place to assign responsibilities and specific actions to support increased grounds for confidence that the security controls in the information system are implemented correctly and operating as intended.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE):* Policies, procedures, records, documents, or activities related to assigning responsibilities and specific actions for security control implementation and operation. (L) **Interview** (DEPTH, COVERAGE):* Organizational personnel directly involved in assigning responsibilities and specific actions for security control development and implementation. (L) (M) * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.
EAP.3	**ASSESSMENT OBJECTIVE:** *Determine if the organization produces and makes available as part of its normal development and implementation processes, the necessary documentation and records to support increased grounds for confidence that the security controls in the information system are implemented correctly and operating as intended.* (L) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE):* Policies, procedures, records, and documents related to producing and making available documentation and records for security control implementation and operation. (L) * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.

STEP NO.	EXTENDED ASSESSMENT PROCEDURE
EAP.4	**ASSESSMENT OBJECTIVE:** *Determine if the organization takes actions to improve the effectiveness of the security controls in the information system.* (L) (M) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE):* Policies, procedures, records, documents, mechanisms, or activities related to taking corrective actions on security controls that exhibit weaknesses or deficiencies. (L) (M) **Interview** (DEPTH, COVERAGE):* Organizational personnel directly involved in taking corrective actions on security controls that exhibit weaknesses or deficiencies. (L) (M) * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.
EAP.5	**ASSESSMENT OBJECTIVE:** *Determine if the organization applies security controls consistently across the information system to further support increased grounds for confidence that the controls are implemented correctly and operating as intended.* (L) (M) **ASSESSMENT METHODS AND OBJECTS:** **Examine** (DEPTH, COVERAGE):* Policies, procedures, records, documents, mechanisms, or activities related to security control implementation and operation. (L) (M) **Interview** (DEPTH, COVERAGE):* Organizational personnel directly involved in security control implementation and operation. (L) (M) * For each assessment method used in an assessment procedural step, assessors must apply the appropriate values for the depth and coverage attributes in accordance with the impact level of the information system. See Appendices D and E.

APPENDIX G

PENETRATION TESTING

ASSESSMENT TOOLS AND TECHNIQUES TO IDENTIFY INFORMATION SYSTEM WEAKNESSES

Organizations should consider adding controlled penetration testing to their arsenal of tools and techniques used to assess the security controls in the information system. Penetration testing is a specific type of assessment methodology in which assessors simulate the actions of a given class of attacker by using a defined set of documentation (that is, the documentation representative of what that class of attacker is likely to possess) and working under other specific constraints to attempt to circumvent the security features of an information system. Penetration testing is conducted as a controlled attempt to breach the security controls employed within the information system using the attacker's techniques and appropriate hardware and software tools. Penetration testing represents the results of a specific assessor or group of assessors at a specific point in time using agreed-upon *rules of engagement*. As such, and considering the complexity of the information technologies commonly employed by organizations today, penetration testing should be viewed not as a means to verify the security of an information system, but rather as a means to: (i) enhance the organization's understanding of the system; (ii) uncover some weaknesses or deficiencies in the system; and (iii) indicate the level of effort required on the part of adversaries to breach the system safeguards.[37]

Keeping in mind reasonable expectations toward penetration testing results, organizations should consider performing controlled penetration testing on moderate-impact and high-impact information systems. Penetration testing exercises can be scheduled and/or random in accordance with organizational policy and organizational assessments of risk. Consideration should be given to performing penetration tests: (i) on any newly developed information system (or legacy system undergoing a major upgrade) before the system is authorized for operation; (ii) after important changes are made to the environment in which the information system operates; and (iii) when a new type of attack is discovered that may impact the system. Organizations actively monitor the information systems environment and the threat landscape (e.g., new vulnerabilities, attack techniques, new technology deployments, user security awareness and training) to identify changes that require out-of-cycle penetration testing.

The organization specifies which information system components are subject to penetration testing and the attacker's profile to be adopted throughout the penetration testing exercises. The organization trains selected personnel in the use and maintenance of penetration testing tools and techniques. Effective penetration testing tools should have the capability to readily update the list of attack techniques and exploitable vulnerabilities used during the exercises. Organizations should update the list of attack techniques and exploitable vulnerabilities used in penetration testing in accordance with an organizational assessment of risk or when significant new vulnerabilities or threats are identified and reported. Whenever possible, organizations should employ tools and attack techniques that include the capability to perform penetration testing exercises on information systems and security controls in an automated manner.

The information obtained from the penetration testing process should be shared with appropriate personnel throughout the organization to help prioritize the vulnerabilities in the information

[37] The failure of an assessor or group of assessors to penetrate an information system may be more indicative of team expertise, resources applied, or hindrance by rules of engagement than a statement of overall system security.

system that are demonstrably subject to compromise by attackers of a profile equivalent to the ones used in the penetration testing exercises. The prioritization helps to determine effective strategies for eliminating the identified vulnerabilities and mitigating associated risks to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the operation and use of the information system. Penetration testing should be integrated into the network security testing process and the patch and vulnerability management process. NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Penetration Testing Considerations

Organization should consider the following in developing and implementing a controlled penetration testing program:

- An effective penetration test goes beyond vulnerability scanning, to provide an explicit and often dramatic proof of mission risks and an indicator of the level of effort an adversary would need to expend in order to cause harm to the organization's operations and assets, to individuals, to other organizations, or to the nation;
- An effective penetration test approaches the information system as the adversary would, considering vulnerabilities, incorrect system configurations, trust relationships between organizations, and architectural weaknesses in the environment under test;
- An effective penetration test has a clearly defined scope and contains as a minimum:
  - A definition of the environment subject to test (e.g., facilities, users, organizational groups, etc.);
  - A definition of the attack surface to be tested (e.g., servers, desktop systems, wireless networks, web applications, intrusion detection and prevention systems, firewalls, email accounts, user security awareness and training posture, incident response posture, etc.);
  - A definition of the threat sources to simulate (e.g., an enumeration of attacker's profiles to be used: internal attacker, casual attacker, single or group of external targeted attackers, criminal organization, etc.);
  - A definition of level of effort (time and resources) to be expended; and
  - A definition of the rules of engagement.
- An effective penetration test thoroughly documents all activities performed during the test, including all exploited vulnerabilities, and how the vulnerabilities were combined into attacks;
- An effective penetration test produces results indicating a risk level for a given attacker by using the level of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system;
- An effective penetration test validates existing security controls (including risk mitigation mechanisms such as firewalls, intrusion detection and prevention systems);
- An effective penetration test provides a verifiable and reproducible log of all the activities performed during the test; and
- An effective penetration test provides actionable results with information about possible remediation measures for the successful attacks performed.

APPENDIX H

ASSESSMENT PROCEDURE SELECTION WORK SHEET

SELECTING THE BASE SET OF ASSESSMENT PROCEDURES FOR TAILORING

The work sheet provided in this appendix summarizes all of the specialized assessment procedures and associated procedural steps listed in Appendix F (Assessment Procedure Catalog) by NIST Special Publication 800-53 security control/control enhancement identifier. This work sheet is intended to assist users of this document in identifying and selecting the base set of procedures for assessing the information system security controls. The base set of assessment procedures requires *tailoring* as appropriate (see Section 3.3) to reflect the security controls defined and documented in the organization's information system security plan and to support the type of security assessment being conducted. The first column of the work sheet can be used by organizations to identify the security controls and security control enhancements that are contained in the security plan for the information system. The second column can be used to identify which security controls are part of the current assessment if the organization is conducting a partial assessment (for example, conducting an assessment as part of continuous monitoring where a subset of the security controls are assessed on an ongoing basis). The third and fourth columns list all of the security controls (and control enhancements) in Special Publication 800-53 by shorthand identifier and formal control name, respectively. The fifth and final column lists all of the procedural steps for each assessment procedure in Appendix F (i.e., the procedural steps associated with each security control and control enhancement). The set of procedures to be tailored and used in assessing the security controls in the organizational information system correspond to the security controls and security control enhancements checked in the first column (or second column for partial assessments). Assessment procedures developed for the assessment of organization-specific or system-specific controls not listed in Appendix F must also be executed. A section of the work sheet is reserved for listing these additional security controls.

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
Access Control				
		AC-1	Access Control Policy and Procedures	AC-1.1, AC-1.2
		AC-2	Account Management	AC-2.1
		AC-2(1)	Account Management	AC-2(1).1
		AC-2(2)	Account Management	AC-2(2).1
		AC-2(3)	Account Management	AC-2(3).1
		AC-2(4)	Account Management	AC-2(4).1
		AC-3	Access Enforcement	AC-3.1
		AC-3(1)	Access Enforcement	AC-3(1).1
		AC-4	Information Flow Enforcement	AC-4.1, AC-4.2
		AC-4(1)	Information Flow Enforcement	AC-4(1).1
		AC-4(2)	Information Flow Enforcement	AC-4(2).1
		AC-4(3)	Information Flow Enforcement	AC-4(3).1
		AC-5	Separation of Duties	AC-5.1
		AC-6	Least Privilege	AC-6.1
		AC-7	Unsuccessful Login Attempts	AC-7.1
		AC-7(1)	Unsuccessful Login Attempts	AC-7(1).1
		AC-8	System Use Notification	AC-8.1
		AC-9	Previous Logon Notification	AC-9.1
		AC-10	Concurrent Session Control	AC-10.1
		AC-11	Session Lock	AC-11.1
		AC-12	Session Termination	AC-12.1
		AC-12(1)	Session Termination	AC-12(1).1
		AC-13	Supervision and Review—Access Control	AC-13.1
		AC-13(1)	Supervision and Review—Access Control	AC-13(1).1
		AC-14	Permitted Actions w/o Identification or Authentication	AC-14.1
		AC-14(1)	Permitted Actions w/o Identification or Authentication	AC-14(1).1
		AC-15	Automated Marking	AC-15.1
		AC-16	Automated Labeling	AC-16.1
		AC-17	Remote Access	AC-17.1
		AC-17(1)	Remote Access	AC-17(1).1
		AC-17(2)	Remote Access	AC-17(2).1
		AC-17(3)	Remote Access	AC-17(3).1
		AC-17(4)	Remote Access	AC-17(4).1
		AC-18	Wireless Access Restrictions	AC-18.1
		AC-18(1)	Wireless Access Restrictions	AC-18(1).1
		AC-18(2)	Wireless Access Restrictions	AC-18(2).1
		AC-19	Access Control for Portable and Mobile Devices	AC-19.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		AC-20	Use of External Information Systems	AC-20.1
		AC-20(1)	Use of External Information Systems	AC-20(1).1
Awareness and Training				
		AT-1	Security Awareness and Training Policy and Procedures	AT-1.1, AT-1.2
		AT-2	Security Awareness	AT-2.1
		AT-3	Security Training	AT-3.1
		AT-4	Security Training Records	AT-4.1
		AT-5	Contacts with Security Groups and Associations	AT-5.1
Audit and Accountability				
		AU-1	Audit and Accountability Policy and Procedures	AU-1.1, AU-1.2
		AU-2	Auditable Events	AU-2.1
		AU-2(1)	Auditable Events	AU-2(1).1
		AU-2(2)	Auditable Events	AU-2(2).1
		AU-2(3)	Auditable Events	AU-2(3).1
		AU-3	Content of Audit Records	AU-3.1
		AU-3(1)	Content of Audit Records	AU-3(1).1
		AU-3(2)	Content of Audit Records	AU-3(2).1
		AU-4	Audit Storage Capacity	AU-4.1
		AU-5	Response to Audit Processing Failures	AU-5.1
		AU-5(1)	Response to Audit Processing Failures	AU-5(1).1
		AU-5(2)	Response to Audit Processing Failures	AU-5(2).1
		AU-6	Audit Monitoring, Analysis, and Reporting	AU-6.1, AU-6.2
		AU-6(1)	Audit Monitoring, Analysis, and Reporting	AU-6(1).1
		AU-6(2)	Audit Monitoring, Analysis, and Reporting	AU-6(2).1
		AU-7	Audit Reduction and Report Generation	AU-7.1
		AU-7(1)	Audit Reduction and Report Generation	AU-7(1).1
		AU-8	Time Stamps	AU-8.1
		AU-8(1)	Time Stamps	AU-8(1).1
		AU-9	Protection of Audit Information	AU-9.1
		AU-9(1)	Protection of Audit Information	AU-9(1).1
		AU-10	Non-repudiation	AU-10.1
		AU-11	Audit Record Retention	AU-11.1
Certification, Accreditation, and Security Assessments				
		CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1.1, CA-1.2
		CA-2	Security Assessments	CA-2.1
		CA-3	Information System Connections	CA-3.1
		CA-4	Security Certification	CA-4.1
		CA-4(1)	Security Certification	CA-4(1).1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		CA-5	Plan of Action and Milestones	CA-5.1
		CA-6	Security Accreditation	CA-6.1
		CA-7	Continuous Monitoring	CA-7.1, CA-7.2
		CA-7(1)	Continuous Monitoring	CA-7(1).1
Configuration Management				
		CM-1	Configuration Management Policy and Procedures	CM-1.1, CM-1.2
		CM-2	Baseline Configuration	CM-2.1
		CM-2(1)	Baseline Configuration	CM-2(1).1
		CM-2(2)	Baseline Configuration	CM-2(2).1
		CM-3	Configuration Change Control	CM-3.1
		CM-3(1)	Configuration Change Control	CM-3(1).1
		CM-4	Monitoring Configuration Changes	CM-4.1
		CM-5	Access Restrictions for Change	CM-5.1
		CM-5(1)	Access Restrictions for Change	CM-5(1).1
		CM-6	Configuration Settings	CM-6.1
		CM-6(1)	Configuration Settings	CM-6(1).1
		CM-7	Least Functionality	CM-7.1
		CM-7(1)	Least Functionality	CM-7(1).1
		CM-8	Information System Component Inventory	CM-8.1
		CM-8(1)	Information System Component Inventory	CM-8(1).1
		CM-8(2)	Information System Component Inventory	CM-8(2).1
Contingency Planning				
		CP-1	Contingency Planning Policy and Procedures	CP-1.1, CP-1.2
		CP-2	Contingency Plan	CP-2.1, CP-2.2
		CP-2(1)	Contingency Plan	CP-2(1).1
		CP-2(2)	Contingency Plan	CP-2(2).1
		CP-3	Contingency Training	CP-3.1, CP-3.2
		CP-3(1)	Contingency Training	CP-3(1).1
		CP-3(2)	Contingency Training	CP-3(2).1
		CP-4	Contingency Plan Testing and Exercises	CP-4.1, CP-4.2
		CP-4(1)	Contingency Plan Testing and Exercises	CP-4(1).1
		CP-4(2)	Contingency Plan Testing and Exercises	CP-4(2).1
		CP-4(3)	Contingency Plan Testing and Exercises	CP-4(3).1
		CP-5	Contingency Plan Update	CP-5.1, CP-5.2
		CP-6	Alternate Storage Site	CP-6.1, CP-6.2
		CP-6(1)	Alternate Storage Site	CP-6(1).1
		CP-6(2)	Alternate Storage Site	CP-6(2).1
		CP-6(3)	Alternate Storage Site	CP-6(3).1
		CP-7	Alternate Processing Site	CP-7.1, CP-7.2

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		CP-7(1)	Alternate Processing Site	CP-7(1).1
		CP-7(2)	Alternate Processing Site	CP-7(2).1
		CP-7(3)	Alternate Processing Site	CP-7(3).1
		CP-7(4)	Alternate Processing Site	CP-7(4).1, CP-7(4).2
		CP-8	Telecommunications Services	CP-8.1, CP-8.2
		CP-8(1)	Telecommunications Services	CP-8(1).1
		CP-8(2)	Telecommunications Services	CP-8(2).1
		CP-8(3)	Telecommunications Services	CP-8(3).1
		CP-8(4)	Telecommunications Services	CP-8(4).1
		CP-9	Information System Backup	CP-9.1, CP-9.2
		CP-9(1)	Information System Backup	CP-9(1).1
		CP-9(2)	Information System Backup	CP-9(2).1
		CP-9(3)	Information System Backup	CP-9(3).1
		CP-9(4)	Information System Backup	CP-9(4).1
		CP-10	Information System Recovery and Reconstitution	CP-10.1, CP-10.2
		CP-10(1)	Information System Recovery and Reconstitution	CP-10(1).1
Identification and Authentication				
		IA-1	Identification and Authentication Policy and Procedures	IA-1.1, IA-1.2
		IA-2	User Identification and Authentication	IA-2.1
		IA-2(1)	User Identification and Authentication	IA-2(1).1
		IA-2(2)	User Identification and Authentication	IA-2(2).1
		IA-2(3)	User Identification and Authentication	IA-2(3).1
		IA-3	Device Identification and Authentication	IA-3.1
		IA-4	Identifier Management	IA-4.1, IA-4.2
		IA-5	Authenticator Management	IA-5.1
		IA-6	Authenticator Feedback	IA-6.1
		IA-7	Cryptographic Module Authentication	IA-7.1
Incident Response				
		IR-1	Incident Response Policy and Procedures	IR-1.1, IR-1.2
		IR-2	Incident Response Training	IR-2.1
		IR-2(1)	Incident Response Training	IR-2(1).1
		IR-2(2)	Incident Response Training	IR-2(2).1
		IR-3	Incident Response Testing and Exercises	IR-3.1
		IR-3(1)	Incident Response Testing and Exercises	IR-3(1).1
		IR-4	Incident Handling	IR-4.1
		IR-4(1)	Incident Handling	IR-4(1).1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		IR-5	Incident Monitoring	IR-5.1
		IR-5(1)	Incident Monitoring	IR-5(1).1
		IR-6	Incident Reporting	IR-6.1
		IR-6(1)	Incident Reporting	IR-6(1).1
		IR-7	Incident Response Assistance	IR-7.1
		IR-7(1)	Incident Response Assistance	IR-7(1).1
Maintenance				
		MA-1	System Maintenance Policy and Procedures	MA-1.1, MA-1.2
		MA-2	Controlled Maintenance	MA-2.1
		MA-2(1)	Controlled Maintenance	MA-2(1).1
		MA-2(2)	Controlled Maintenance	MA-2(2).1
		MA-3	Maintenance Tools	MA-3.1
		MA-3(1)	Maintenance Tools	MA-3(1).1
		MA-3(2)	Maintenance Tools	MA-3(2).1
		MA-3(3)	Maintenance Tools	MA-3(3).1
		MA-3(4)	Maintenance Tools	MA-3(4).1
		MA-4	Remote Maintenance	MA-4.1
		MA-4(1)	Remote Maintenance	MA-4(1).1
		MA-4(2)	Remote Maintenance	MA-4(2).1
		MA-4(3)	Remote Maintenance	MA-4(3).1
		MA-5	Maintenance Personnel	MA-5.1
		MA-6	Timely Maintenance	MA-6.1
Media Protection				
		MP-1	Media Protection Policy and Procedures	MP-1.1, MP-1.2
		MP-2	Media Access	MP-2.1
		MP-2(1)	Media Access	MP-2(1).1
		MP-3	Media Labeling	MP-3.1
		MP-4	Media Storage	MP-4.1
		MP-5	Media Transport	MP-5.1
		MP-5(1)	Media Transport	MP-5(1).1
		MP-5(2)	Media Transport	MP-5(2).1
		MP-5(3)	Media Transport	MP-5(3).1
		MP-6	Media Sanitization and Disposal	MP-6.1
		MP-6(1)	Media Sanitization and Disposal	MP-6(1).1
		MP-6(2)	Media Sanitization and Disposal	MP-6(2).1
Physical and Environmental Protection				
		PE-1	Physical and Environmental Protection Policy and Procedures	PE-1.1, PE-1.2
		PE-2	Physical Access Authorizations	PE-2.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		PE-3	Physical Access Control	PE-3.1, PE-3.2, PE-3.3
		PE-3(1)	Physical Access Control	PE-3(1).1
		PE-4	Access Control for Transmission Medium	PE-4.1
		PE-5	Access Control for Display Medium	PE-5.1
		PE-6	Monitoring Physical Access	PE-6.1
		PE-6(1)	Monitoring Physical Access	PE-6(1).1
		PE-6(2)	Monitoring Physical Access	PE-6(2).1
		PE-7	Visitor Control	PE-7.1
		PE-7(1)	Visitor Control	PE-7(1).1
		PE-8	Access Records	PE-8.1
		PE-8(1)	Access Records	PE-8(1).1
		PE-8(2)	Access Records	PE-8(2).1
		PE-9	Power Equipment and Power Cabling	PE-9.1
		PE-9(1)	Power Equipment and Power Cabling	PE-9(1).1
		PE-10	Emergency Shutoff	PE-10.1
		PE-10(1)	Emergency Shutoff	PE-10(1).1
		PE-11	Emergency Power	PE-11.1
		PE-11(1)	Emergency Power	PE-11(1).1
		PE-11(2)	Emergency Power	PE-11(2).1
		PE-12	Emergency Lighting	PE-12.1
		PE-13	Fire Protection	PE-13.1
		PE-13(1)	Fire Protection	PE-13(1).1
		PE-13(2)	Fire Protection	PE-13(2).1
		PE-13(3)	Fire Protection	PE-13(3).1
		PE-14	Temperature and Humidity Controls	PE-14.1
		PE-15	Water Damage Protection	PE-15.1
		PE-15(1)	Water Damage Protection	PE-15(1).1
		PE-16	Delivery and Removal	PE-16.1
		PE-17	Alternate Work Site	PE-17.1
		PE-18	Location of Information System Components	PE-18.1
		PE-18(1)	Location of Information System Components	PE-18(1).1
		PE-19	Information Leakage	PE-19.1
Planning				
		PL-1	Security Planning Policy and Procedures	PL-1.1, PL-1.2
		PL-2	System Security Plan	PL-2.1
		PL-3	System Security Plan Update	PL-3.1
		PL-4	Rules of Behavior	PL-4.1
		PL-5	Privacy Impact Assessment	PL-5.1
		PL-6	Security-Related Activity Planning	PL-6.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
Personnel Security				
		PS-1	Personnel Security Policy and Procedures	PS-1.1, PS-1.2
		PS-2	Position Categorization	PS-2.1
		PS-3	Personnel Screening	PS-3.1
		PS-4	Personnel Termination	PS-4.1
		PS-5	Personnel Transfer	PS-5.1
		PS-6	Access Agreements	PS-6.1
		PS-7	Third-Party Personnel Security	PS-7.1
		PS-8	Personnel Sanctions	PS-8.1
Risk Assessment				
		RA-1	Risk Assessment Policy and Procedures	RA-1.1, RA-1.2
		RA-2	Security Categorization	RA-2.1
		RA-3	Risk Assessment	RA-3.1
		RA-4	Risk Assessment Update	RA-4.1
		RA-5	Vulnerability Scanning	RA-5.1
		RA-5(1)	Vulnerability Scanning	RA-5(1).1
		RA-5(2)	Vulnerability Scanning	RA-5(2).1
		RA-5(3)	Vulnerability Scanning	RA-5(3).1
System and Services Acquisition				
		SA-1	System and Services Acquisition Policy and Procedures	SA-1.1, SA-1.2
		SA-2	Allocation of Resources	SA-2.1
		SA-3	Life Cycle Support	SA-3.1
		SA-4	Acquisitions	SA-4.1
		SA-4(1)	Acquisitions	SA-4(1).1
		SA-4(2)	Acquisitions	SA-4(2).1
		SA-5	Information System Documentation	SA-5.1
		SA-5(1)	Information System Documentation	SA-5(1).1
		SA-5(2)	Information System Documentation	SA-5(2).1
		SA-6	Software Usage Restrictions	SA-6.1
		SA-7	User Installed Software	SA-7.1
		SA-8	Security Engineering Principles	SA-8.1
		SA-9	External Information System Services	SA-9.1
		SA-10	Developer Configuration Management	SA-10.1
		SA-11	Developer Security Testing	SA-11.1
System and Communications Protection				
		SC-1	System and Communications Protection Policy and Procedures	SC-1.1, SC-1.2
		SC-2	Application Partitioning	SC-2.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		SC-3	Security Function Isolation	SC-3.1
		SC-3(1)	Security Function Isolation	SC-3(1).1
		SC-3(2)	Security Function Isolation	SC-3(2).1
		SC-3(3)	Security Function Isolation	SC-3(3).1
		SC-3(4)	Security Function Isolation	SC-3(4).1
		SC-3(5)	Security Function Isolation	SC-3(5).1
		SC-4	Information Remnance	SC-4.1
		SC-5	Denial of Service Protection	SC-5.1
		SC-5(1)	Denial of Service Protection	SC-5(1).1
		SC-5(2)	Denial of Service Protection	SC-5(2).1
		SC-6	Resource Priority	SC-6.1
		SC-7	Boundary Protection	SC-7.1
		SC-7(1)	Boundary Protection	SC-7(1).1
		SC-7(2)	Boundary Protection	SC-7(2).1
		SC-7(3)	Boundary Protection	SC-7(3).1
		SC-7(4)	Boundary Protection	SC-7(4).1
		SC-7(5)	Boundary Protection	SC-7(5).1
		SC-7(6)	Boundary Protection	SC-7(6).1
		SC-8	Transmission Integrity	SC-8.1
		SC-8(1)	Transmission Integrity	SC-8(1).1
		SC-9	Transmission Confidentiality	SC-9.1
		SC-9(1)	Transmission Confidentiality	SC-9(1).1
		SC-10	Network Disconnect	SC-10.1
		SC-11	Trusted Path	SC-11.1
		SC-12	Cryptographic Key Establishment and Management	SC-12.1
		SC-13	Use of Cryptography	SC-13.1
		SC-14	Public Access Protections	SC-14.1
		SC-15	Collaborative Computing	SC-15.1
		SC-15(1)	Collaborative Computing	SC-15(1).1
		SC-16	Transmission of Security Parameters	SC-16.1
		SC-17	Public Key Infrastructure Certificates	SC-17.1
		SC-18	Mobile Code	SC-18.1
		SC-19	Voice Over Internet Protocol	SC-19.1
		SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20.1
		SC-20(1)	Secure Name /Address Resolution Service (Authoritative Source)	SC-20(1).1
		SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
		SC-21(1)	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21(1).1
		SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22.1
		SC-23	Session Authenticity	SC-23.1
System and Information Integrity				
		SI-1	System and Information Integrity Policy and Procedures	SI-1.1, SI-1.2
		SI-2	Flaw Remediation	SI-2.1
		SI-2(1)	Flaw Remediation	SI-2(1).1
		SI-2(2)	Flaw Remediation	SI-2(2).1
		SI-3	Malicious Code Protection	SI-3.1
		SI-3(1)	Malicious Code Protection	SI-3(1).1
		SI-3(2)	Malicious Code Protection	SI-3(2).1
		SI-4	Information System Monitoring Tools and Techniques	SI-4.1
		SI-4(1)	Information System Monitoring Tools and Techniques	SI-4(1).1
		SI-4(2)	Information System Monitoring Tools and Techniques	SI-4(2).1
		SI-4(3)	Information System Monitoring Tools and Techniques	SI-4(3).1
		SI-4(4)	Information System Monitoring Tools and Techniques	SI-4(4).1
		SI-4(5)	Information System Monitoring Tools and Techniques	SI-4(5).1
		SI-5	Security Alerts and Advisories	SI-5.1
		SI-5(1)	Security Alerts and Advisories	SI-5(1).1
		SI-6	Security Functionality Verification	SI-6.1
		SI-6(1)	Security Functionality Verification	SI-6(1).1
		SI-6(2)	Security Functionality Verification	SI-6(2).1
		SI-7	Software and Information Integrity	SI-7.1
		SI-7(1)	Software and Information Integrity	SI-7(1).1
		SI-7(2)	Software and Information Integrity	SI-7(2).1
		SI-7(3)	Software and Information Integrity	SI-7(3).1
		SI-8	Spam Protection	SI-8.1
		SI-8(1)	Spam Protection	SI-8(1).1
		SI-8(2)	Spam Protection	SI-8(2).1
		SI-9	Information Input Restrictions	SI-9.1
		SI-10	Information Accuracy, Completeness, Validity, and Authenticity	SI-10.1
		SI-11	Error Handling	SI-11.1
		SI-12	Information Output Handling and Retention	SI-12.1

SECURITY PLAN	CURRENT ASSESSMENT	CONTROL NUMBER	CONTROL NAME	ASSESSMENT PROCEDURAL STEPS
Additional Security Controls Not Contained in NIST Special Publication 800-53				

APPENDIX I

MANAGING ASSESSMENT RESULTS

AN APPROACH FOR DOCUMENTING ASSESSMENT FINDINGS

This appendix provides an approach for managing assessment results produced during security assessments. The security assessment determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the security assessment, including the findings of the assessor and recommendations for correcting any weaknesses or deficiencies in the security controls, are documented in the security assessment report. The primary purpose of the security assessment report is to convey the results of the security assessment to appropriate organizational officials.[38]

Key Elements for Assessment Reporting

The following elements should be included in security assessment reports:

- *Information System Name and Impact Level*
- *Site(s) Assessed and Assessment Date(s)*
- *Security Control or Control Enhancement and Associated Supplemental Guidance*
- *For Each Assessment Procedural Step:*
  - *Assessment Objective (determination statements)*
  - *Assessment Methods and Objects*
  - *Assessment Finding Summary (indicating satisfied or other than satisfied)*
- *Assessor Comments (deficiencies or weaknesses noted)*
- *Assessor Recommendations (remediation, corrective actions, or improvements)*

[38] The security assessment report is included in the security accreditation package along with the information system security plan (including updated risk assessment) and the plan of action and milestones to provide authorizing officials with the information necessary to make credible, risk-based decisions on whether to place an information system into operation or continue its operation. As the security certification and accreditation process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the system development life cycle, the ability to update the security assessment report frequently becomes a critical aspect of an information security program. It is important to emphasize the relationship, described in NIST Special Publication 800-37, among the three key documents in the accreditation package (i.e., the system security plan including risk assessment, the security assessment report, and the plan of action and milestones). It is these documents that provide the best indication of the overall security status of the information system and the ability of the system to protect, to the degree necessary, the organization's operations and assets, individuals, other organizations, and the nation. Updates to these key documents should be provided on an ongoing basis in accordance with the continuous monitoring program established by the organization.

The Assessment Findings

Each determination statement executed by an assessor results in one of the following findings: (i) satisfied (S); or (ii) other than satisfied (O). Consider the following example for security control CP-1. The assessment procedure for CP-1 consists of two procedural steps denoted CP-1.1 and CP-1.2. The assessor initially executes the determination statements in the CP-1.1 procedural step and produces the following findings:

CP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents contingency planning policy and procedures;* **(S)** *(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;* **(O)** *(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and* **(S)** *(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.* **(O)** **Comments and Recommendations:** CP-1.1(ii) is marked as *other than satisfied* because there was insufficient evidence to determine if the following two of the ten identified organizational elements on the distribution list for the contingency planning policy and procedures actually had received the policy and procedures: (i) organization physical security office; and (ii) organization finance and accounting office. Straightforward remediation action recommended of providing necessary documentation to the two organizational elements not receiving the policy and procedures. CP-1.1 (iv) is marked as *other than satisfied* because over fifty percent of the contingency planning policy and procedure documents identified as requiring updates had not in fact been updated. Significant remediation action is recommended to correct clear process deficiencies.

In a similar manner, the assessor executes the determination statements in the CP-1.2 procedural step and produces the following findings:

CP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;* **(S)** *(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and* **(S)** *(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.* **(O)** **Comments and Recommendations:** CP-1.2(iii) is marked as *other than satisfied* because the assessment team could not make a determination. The entire suite of updated contingency planning procedures (identified in CP-1.1(iv) finding) was unavailable and therefore, the sufficiency of contingency planning policy coverage could not be determined. Further investigation is needed.

Sample Security Assessment Reporting Form

This sample reporting format is illustrative and not intended to limit organizational flexibility in determining the most appropriate presentation for the purposes of a given security assessment.

SECURITY ASSESSMENT REPORTING FORM	
SECTION I: INFORMATION SYSTEM AND ASSESSMENT INFORMATION	
Information System Name	**Impact Level** *(low, moderate, high)*
Site(s) Assessed	**Assessment Date(s)**
SECTION II: SECURITY CONTROL INFORMATION	
Security Control or Control Enhancement *(Insert text from security control or control enhancement being assessed as stated in, or as referenced by the approved information system security plan.)*	
Supplemental Guidance Associated with Security Control or Control Enhancement *(Insert text from the supplemental guidance from the security control or control enhancement being assessed as stated in, or as referenced by the approved information system security plan.)*	
SECTION III: ASSESSMENT FINDINGS	
Assessment Procedural Step *(Identify assessment procedural step, e.g., CP-1.1, associated with the security control or control enhancement described above.)*	
Assessment Objective *(See determination statements below which restate the determinations from the assessment procedural step, as tailored for this security assessment, e.g., including organization-specific information, where appropriate.)*	**Finding** *(S/O)*
Determination statement	
Determination statement	
Determination statement	
Determination statement	
Assessment Methods and Objects *(Identify assessment methods and assessment objects as tailored for this assessment, e.g., the specific version of a specification examined or the nature of the examination performed.)*	

SECURITY ASSESSMENT REPORTING FORM
SECTION IV: ASSESSOR COMMENTS AND RECOMMENDATIONS
Assessor Comments *(Explanation of weaknesses or deficiencies noted for each finding of other than satisfied.)*
Assessor Recommendations *(Recommendations for remediation, corrective actions, or improvements in security control implementation or operation.)*

APPENDIX J

RISK MANAGEMENT FRAMEWORK

THE ROLE OF SECURITY ASSESSMENTS IN MANAGING ENTERPRISE RISK

This appendix describes the NIST Risk Management Framework (RMF) and how security assessments are an integral component of an organizational information security program and managing enterprise risk. The following RMF activities related to managing risk are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture—

- ***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.
- ***Select*** an initial set of security controls (i.e., security control baseline from Appendix D) for the information system based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply tailoring guidance from NIST Special Publication 800-53, as appropriate, to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.
- ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.[39]
- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.[40]
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize*** information system operation based upon a determination of the risk to organizational operations and assets, to individuals, to other organizations, and to the nation resulting from the operation of the system and the decision that this risk is acceptable.[41]
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

[39] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk.

[40] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

[41] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization of information systems.

Figure J-1 illustrates the activities in the NIST RMF, highlights the specific activities related to security assessments, and denotes the information security standards and guidance documents associated with each activity.

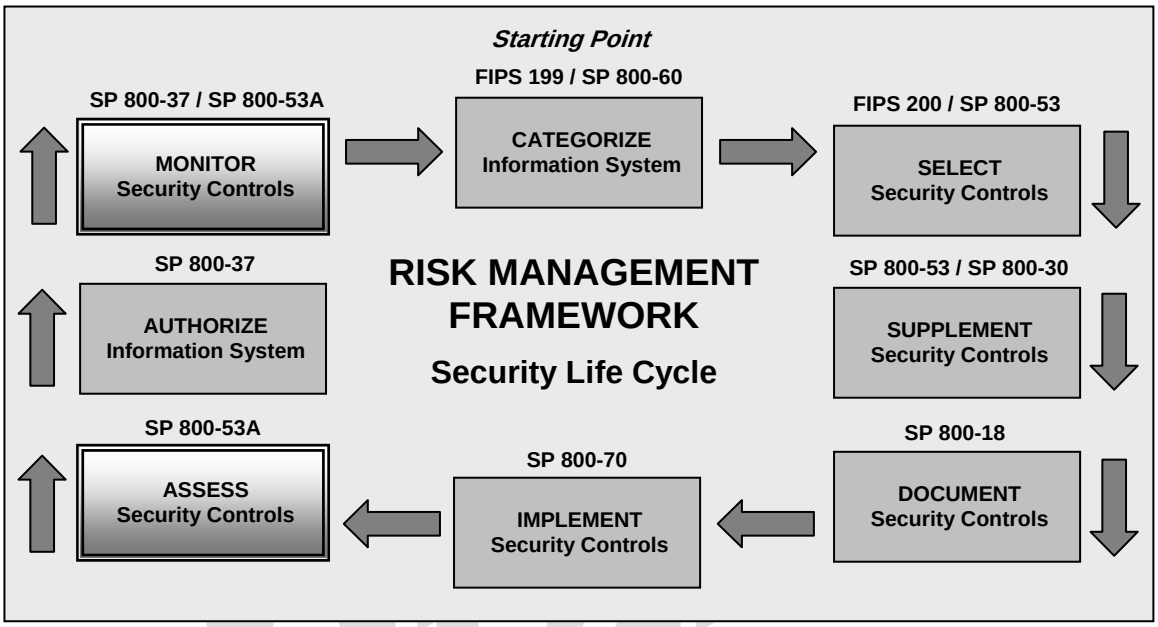

FIGURE J-1: THE RISK MANAGEMENT FRAMEWORK